AdvancedTCA Dual Processor Board

Technical Product Specification

August 2004

Order Number: M8000_TECH_0

Contents

Figures

Tables

Introduction 1

1.1 Document Organization

This document gives technical specifications related to the Intel NetStructure AT8000 High-Performance single Board Computer. The AT8000 is designed following the standards of the Advanced Telecommunications Compute Architecture* (ATCA) Design Guide for high availability, switched network computing. This document is intended for support during system product development and while sustaining a product. It specifies the architecture, design requirements, external requirements, board functionality, and design limitations of the AT8000 Single Board Computer.

The following summarizes the focus of each chapter in this document.

Chapter 1, "Introduction" gives an overview of the information contained in the Kontron AT8000 Technical Product Specification as well as a glossary of acronyms and important terms.

Chapter 2, "Features Overview" introduces the key features of the AT8000. It includes a functional block diagram and a brief description of each block.

Chapter 3, "Hardware Management Overview"provides a high-level overview related to IPMI implementation based on PICMG* 3.0 and IPMI v1.5 specifications in the AT8000 SBC.

Chapter 4, "Connectors" includes an illustration of connector locations, connector descriptions, and pinout tables.

Chapter 5, "Addressing" summarizes the information you need to configure the AT8000. Included are the PCI configuration map, Configuration Address register, Configuration Data register, I/O address assignments, memory map, and IPMC addresses.

Chapter 6, "Specifications" contains the mechanical, environmental, and reliability specifications for the AT8000.

Chapter 7, "BIOS Features" provides an introduction to the Intel/AMI BIOS, and the System Management BIOS, stored in flash memory on the AT8000.

Chapter 9, "BIOS Setup" describes the interactive menu system of the BIOS Setup program. The menu allows a user to configure the BIOS for a given system.

Chapter 8, "Error Messages" lists BIOS error messages, Port 80h POST codes, and bus initialization checkpoints, and provides a brief description of each.

Chapter 10, "Operating the Unit" provides specifics for configuring the AT8000, including BIOS configuration and jumper settings.

Chapter 11, "Maintenance" includes supervision and diagnostics information.

Chapter 13, "Component Technology" lists the major components used on the AT8000.

Chapter 14, "Warranty Information" provides warranty information for Intel® NetStructure™ products.

Chapter 15, "Certifications" provides information on how to contact customer support.

Chapter 15, "Certifications" and Chapter 16, "Agency Information" document the regulatory requirements the AT8000 is designed to meet.

Appendix A, "Reference Documents" provides a list of data sheets, standards, and specifications for the technology designed into the AT8000.

Appendix B, "List of Supported Commands (IPMI v1.5 and PICMG 3.0)"provides lists of commands supported by IPMI v1.5 and PICMG Specification 3.0.

1.2 Glossary

For ease of use, numeric entries are listed first with alpha entries following. Acronyms and terms are then entered in their respective place.

ACPI	Advanced Configuration and Power Interface.
ATCA	Advanced Telecommunications Compute Architecture
BIOS	Basic Input/Output Subsystem. ROM code that initializes the computer and performs some basic functions.
Blade	An assembled PCB card that plugs into a chassis.
DIMM	Dual Inline Memory Module. Small card with memory on it used for AT8000.
DMI	Desktop Management Interface
EEPROM	Electrically Erasable Programmable Read-Only Memory
Fabric Board	A board capable of moving packet data between Node Boards via the ports of the backplane. This is sometimes referred to as a switch.
Fabric Slot	A slot supporting a link port connection to/from each Node Slot and/or out of the chassis.
Hyper-Threading Technology	Allows a single (or dual) physical processor, to appear as two (or quad) logical processors to a Hyper-Threading Technology aware Operating System.
I^2C	Inter-IC [Integrated Circuit]. 2-wire interface commonly used to carry management data.
IBA	Intel® Boot Agent. The Intel Boot Agent is a software product that allows your networked client computer to boot using a program code image supplied by a remote server.
IDE	Integrated Device Electronics. Common, low-cost disk interface.
IPMB	Intelligent Platform Management Bus. Physical 2-wire medium to carry IPMI.
IPMC	Intelligent Platform Management Controller. ASIC in baseboard responsible for low-level system management.

IPMI	Intelligent Platform Management Interface. Programming model for system management.
KCS	Keyboard Controller Style interface.
LPC Bus	Los Pin Count Bus. Legacy I/O bus that replaces ISA and X-bus. See the Low Pin Count (LPC) Interface Specification.
MTBF	Mean Time Between Failure. A reliability measure based on the probability of failure.
NEBS	National Equipment Building Standards. Telco standards for equipment emissions, thermal, shock, contaminants, and fire suppression requirements.
NMI	Non-Maskable Interrupt. Low-level PC interrupt.
Node Board	A board capable of providing and/or receiving packet data to/from a Fabric Board via the ports of the networks. The term is used interchangeably with SBC.
AT8000	Single or dual processor Single Board Computer with Fibre Channel.
MPCBL0002	Single or dual processor Single Board Computer without Fibre Channel.
Node Slot	A slot supporting port connections to/from Fabric Slot(s). A Node slot is intended to accept a Node Board
Physical Port	A port that physically exists. It is supported by one of many physical (PHY) type components.
PMC	PCI Mezzanine Card. IEEE1386 standard for embedded PCI cards. They mount parallel to the SBC.
ROM	Read-Only Memory.
SBC	Single Board Computer. This term is used interchangeably with Node Board.
SEL	System Event Log. Action logged by management controller.
SFP	Small Form Factor Pluggable receptacle for the front panel Fibre Channel interfaces.
SMBus	System Management Bus. Similar to I2C
SMI	System Management Interrupt. Low-level PC interrupt which can be initiated by chipset or management controller. Used to service IPMC or handle things like memory errors.
SMS, SMSC	Standard Microsystems Corporation*
USB	Universal Serial Bus. General-purpose peripheral interconnect, operating at 1-12 Mbps.

Features Overview 2

2.1 Application

The Advanced Telecommunications Compute Architecture* (ATCA) standards define open architecture modular computing components for carrier-grade, communications network infrastructure. The goals of the standards are to enable blade-based modular platforms to be:

- cost effective
- high-density
- high-availability
- scalable

These systems use a fabric I/O network for connecting multiple, independent processor boards, I/O nodes (e.g., line cards), and I/O devices (e.g., storage subsystem).

The AT8000 Single Board Computer (SBC) is designed per the ATCA Design Guide for High Availability, Switched Network Computing. Bulk storage for the system is connected through optional dual Fibre Channel interfaces. The AT8000FXX Single Board Computer (SBC) includes a fiber channel controller. The AT8000NXX Single Board Computer (SBC) does not have the fiber channel controller.

2.2 Functional Description

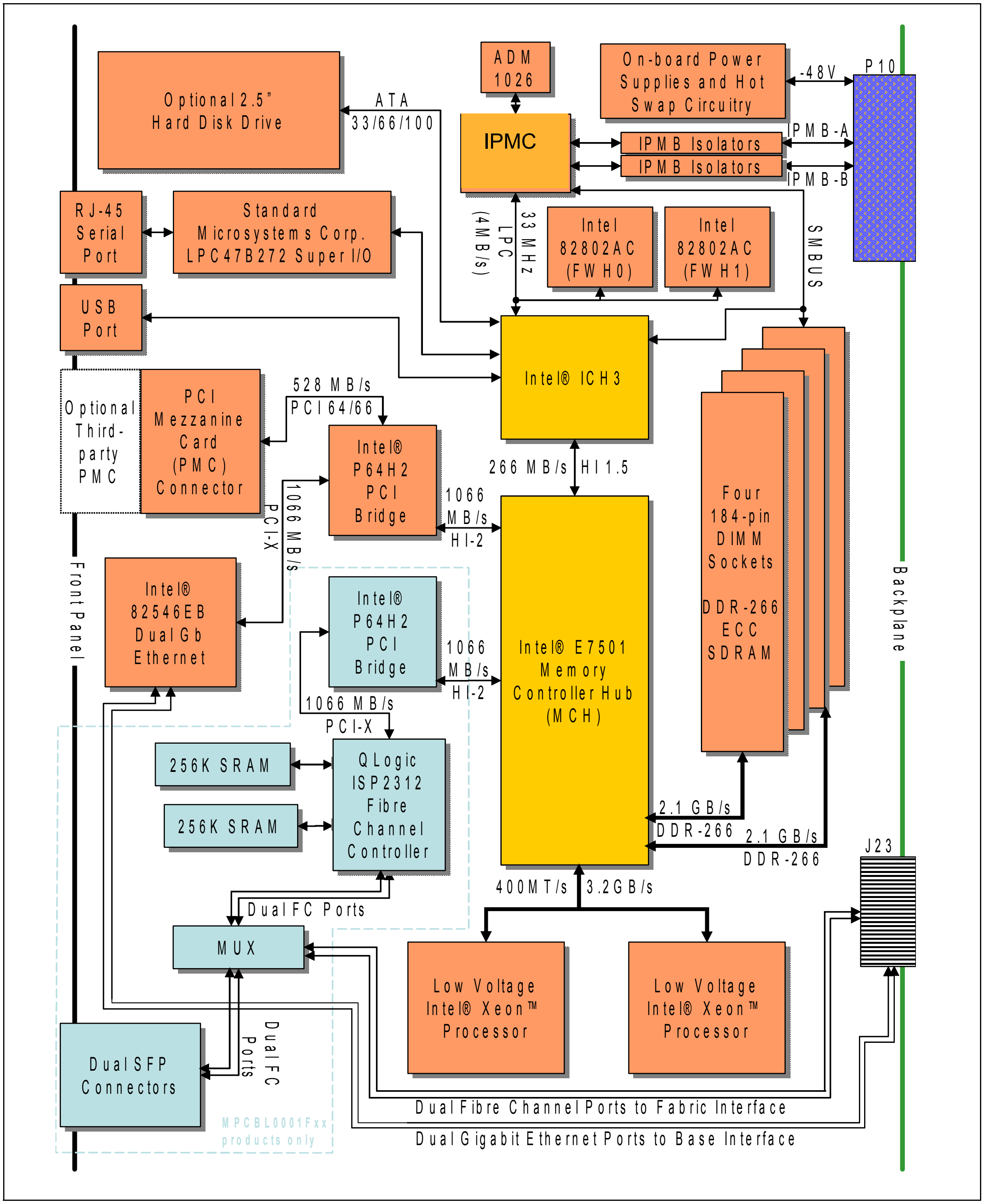
This topic defines the architecture of the AT8000 SBC through descriptions of functional blocks. Figure 1, "AT8000 SBC Block Diagram" on page 14 shows the functional blocks of the AT8000 SBC. The AT8000 SBC is a dual processor, hot-swappable SBC with backplane connections to dual Gigabit Ethernet star networks and dual Fibre Channel star arbitrated loops.

The SBC incorporates an Intelligent Platform Management Controller that monitors critical functions of the board, responds to commands from the shelf manager, and reports events.

Power is supplied to the AT8000 SBC through two redundant -48 V power supply connections. Power for on-board hardware management circuitry is provided through a standby converter on the power mezzanine. This converter, along with all the other converters on the power mezzanine are fed by the diode OR'd -48 V supply from the backplane.

The SBC has provision for the addition of a PMC device and supports 32-bit and 64-bit transfers at 33 MHz and 66 MHz. The SBC also offers one USB and one service terminal interface. An overview of each block follows.

Figure 1. AT8000 SBC Block Diagram



2.2.1 Low Voltage Intel Xeon Processor CPU-0 (U35), CPU-1 (U36)

The AT8000 SBC supports up to two Low Voltage Intel® Xeon™ processors (see Figure 18, “Intel® NetStructure™ AT8000 Component Layout” on page 77 for locations). The Low Voltage Xeon processor incorporates Intel® NetBurst™ microarchitecture and a high-bandwidth Front-Side Bus, allowing performance levels that are significantly higher than previous generations of IA-32 family processors. The processors include the following features:

- 2.0 GHz with a 400 MHz system bus
- 512 Kbyte L2 cache
- Hyper-pipelined technology
- Advanced dynamic execution
- Execution trace cache
- Streaming SIMD (single instruction, multiple data) extensions 2
- Advanced transfer cache
- Enhanced floating point and multimedia engine
- Intel & OEM EEPROM and thermal sensor manageability features
- Supports single and dual processor configurations
- Throttling enabled for protection against high temperatures

The Low Voltage Xeon processor host bus utilizes a split-transaction, deferred-reply protocol. The host bus uses source-synchronous transfer of address and data to improve throughput at the 100 or 133 MHz bus frequency (depending on processor model). Addresses are transferred at 2X the bus frequency while data is transferred at 4X the bus frequency, resulting in peak data transfer rates up to 3.2 or 4.3 GBytes/s.

In addition to the NetBurst microarchitecture, the Low Voltage Intel Xeon processor includes a groundbreaking technology called Hyper-Threading technology. Hyper-Threading technology improves processor performance for multithreaded applications or multitasking environments by supporting multiple software threads on each processor.

Low Voltage Intel Xeon processors require their package case temperatures to be operated below an absolute maximum specification. If the chassis ambient temperature exceeds a level whereby the processor thermal cooling subsystem can no longer maintain the specified case temperature, the processors will automatically enter a mode called Thermal Monitor to reduce their case temperatures. Thermal Monitor controls the processor temperature by modulating the internal processor core clocks, thereby reducing internal power dissipation, and does not require any interaction by the Operating System or Application. Once the case temperatures have reached a safe operating level, the processor will return to its non-modulated operating frequency. See the Low Voltage Intel Xeon processor datasheet, referenced in Appendix A, “Reference Documents”, for further details.

An optional ITP700 port connection is included to facilitate debug and BIOS/software development efforts. This JTAG connection to the processors utilizes voltage-signaling levels that are specific to the Low Voltage Xeon processor family. These levels must not be exceeded or processor damage may occur. Please refer to Intel document ITP700 Debug Port Design Guide, order number 249679-005 for additional information on the ITP connector pin definitions.

2.2.2 Chipset

The Intel® E7501 chipset consists of three major components:

- Intel® E7501 Memory Controller Hub (MCH)
- Intel® 82801CA I/O Controller Hub 3 (ICH3)
- Intel® 82870P2 64-bit PCI/PCI-X Controller Hub 2 (P64H2)

See Figure 18, "Intel® NetStructure™ AT8000 Component Layout" on page 77 for their locations.

2.2.2.1 Intel® E7501 Memory Controller Hub (U22)

The Intel® E7501 Memory Controller Hub (MCH) interfaces between the processor system bus and the memory and I/O subsystems.

Significant features are listed below:

- System/Host Bus Features:
  - Supports dual processors at either 400 or 533 MT/s or a bandwidth of 3.2 or 4.3 GByte/s
  - Supports a 36-bit system bus addressing model
  - 12 deep in-order queue, two deep defer queue
- Memory subsystem features:
  - 144-bit wide (72-bit x 2), DDR-266 memory interfaces with 3.2 or 4.3 GByte/s bandwidth
  - Supports x72, registered DDR-266 ECC DIMMs using 64-, 128-, 256-, and 512-Mbit SDRAMs
  - Supports a maximum of 16 GBytes of memory (AT8000 SBC implementation supports a maximum of 8 Gbytes).
  - Supports S4EC/D4ED ChipKill* ECC (x4 ChipKill)
    - Corrects all bit errors within a single 4-bit nibble
    - Detects all errors contained within two 4-bit nibbles
    - Memory scrubbing supported
  - Supports up to 32 simultaneous open pages
  - Hardware support for auto-initialization of memory with valid ECC
- I/O features:
  - Hub interface A provides HI 1.5 connection for ICH3
    - 266 MB/s data bandwidth with parity protection
    - 8 bits wide, 66 MHz clock, 4x data transfer (quad-pumped)
    - Supports 64-bit inbound addressing, 32-bit outbound addressing
  - Hub interfaces B and C provide HI2.0 connections for two P64H2s
    - 1 GByte/s data bandwidth with ECC protection in each direction
    - 16-bits wide, 66 MHz clock, 8x data transfer (octal pumped)
    - Supports 64-bit inbound, 32-bit outbound addressing

The MCH I/O subsystems interface incorporates four hub interfaces. Each Hub interface is a point-to-point connection between the MCH and an I/O bridge/device. The various components of the chipset communicate via these connected hub interfaces:

- The first hub link connects the MCH to the ICH3.
- The next two hub link interfaces connect the MCH to P64H2 components.
- The remaining hub link is unused.

2.2.2.2 Intel® 82801CA I/O Controller Hub 3 (U7)

The Intel® 82801CA I/O Controller Hub 3 (IHC3) provides the legacy I/O subsystem and integrates advanced I/O functions. ICH3 features are listed below:

- IDE interface controller
- Three Universal Host Controller Interface (UHCI)
- USB host controllers supporting up to 6 ports (AT8000 SBC implementation supports one port on the front panel)
- Integrated I/O APIC
- SMBus 2.0 controller
- LPC interface
- Watchdog timer #3 (see “Watchdog Timers (WDTs)” on page 52)
- PCI 2.2 bus interface supporting 32bit/33 MHz operation
- Connects to MCH through Hub Interface A (HI 1.5)

The AT8000 SBC implements one USB port and does not use the ICH3 PCI connection.

2.2.2.2.1 PCI Bus Master IDE Interface (J24)

The ICH3 acts as a PCI based, enhanced IDE, 32-bit interface controller for intelligent disk drives that have disk controller electronics onboard. The SBC includes a single 40-pin (2 x 20) IDE connector (J24) that supports one master or one slave device. See Figure 18, “Intel® NetStructure™ AT8000 Component Layout” on page 77 drawing for its location. The IDE controller provides support for an internally mounted 2.5” hard disk. The IDE controller has the following features:

- PIO and DMA transfer modes
- Mode 4 timings
- Supports Ultra ATA33/66/100 synchronous DMA
- Buffering for PCI/IDE burst transfers
- Master/slave IDE mode
- Support for up to two devices (Master/Slave) via a single primary IDE connector (AT8000 SBC implementation supports one optional physical 2.5" IDE device)

Note: Incorporating an optional IDE Hard Disk drive may significantly impact the Reliability Specifications in Section 6.3.

Note: Performance of the IDE interface may be impacted by the DMA mode and type of DMA transfers used. Even though the BIOS automatically sets the DMA mode/type, the OS could downgrade the DMA transfer mode. Check the operating system documentation to see what DMA mode is used by default and whether it is possible to change to a higher performance DMA mode.

2.2.2.3 Intel® 82870P2 64-bit PCI/PCI-X Controller Hub 2 (U14, U24)

The two P64H2 devices provide the system's high-performance PCI bus support. See Figure 18, "Intel® NetStructure™ AT8000 Component Layout" on page 77 for their locations. Each P64H2 component supports two independent, 64-bit, PCI/PCI-X interfaces. 32-bit/33 MHz and 64-bit/66 MHz PCI bus modes are also supported. Each PCI bus interface features:

- PCI-X 1.0 Specification compliance
- PCI Specification 2.2 compliance
- PCI-PCI Bridge Rev 1.1 compliance
- PCI Hot Plug 1.0 compliance
- I/O APIC supporting up to 24 interrupts (16 external pins)
- PCI peer-to-peer write capability between PCI ports
- SMBus target for Out-of-Band access to all internal PCI registers

Each of the two P64H2 devices (U14, U24) included on the AT8000 SBC provides the bridge to two independent PCI bus connections, as shown in Table 1, "P64H2 Interfaces" on page 18.

Table 1. P64H2 Interfaces

P64H2 Device	Interface
U24	PCI-X interface to the optional dual Fibre Channel controller
U14	• PCI-X interface to the dual Gigabit Ethernet controller • 64-bit/66 MHz PCI bus for a plug-in PMC card

The two high-speed communications interfaces (Gigabit Ethernet and Fibre Channel) are located in separate P64H2 devices to maximize data throughput. A single HI-2 hub link connection from the P64H2 to the MCH provides a >1 Gbyte/s bandwidth back to memory and the processor System Bus.

2.2.3 Memory (J8, J9, J10, J11)

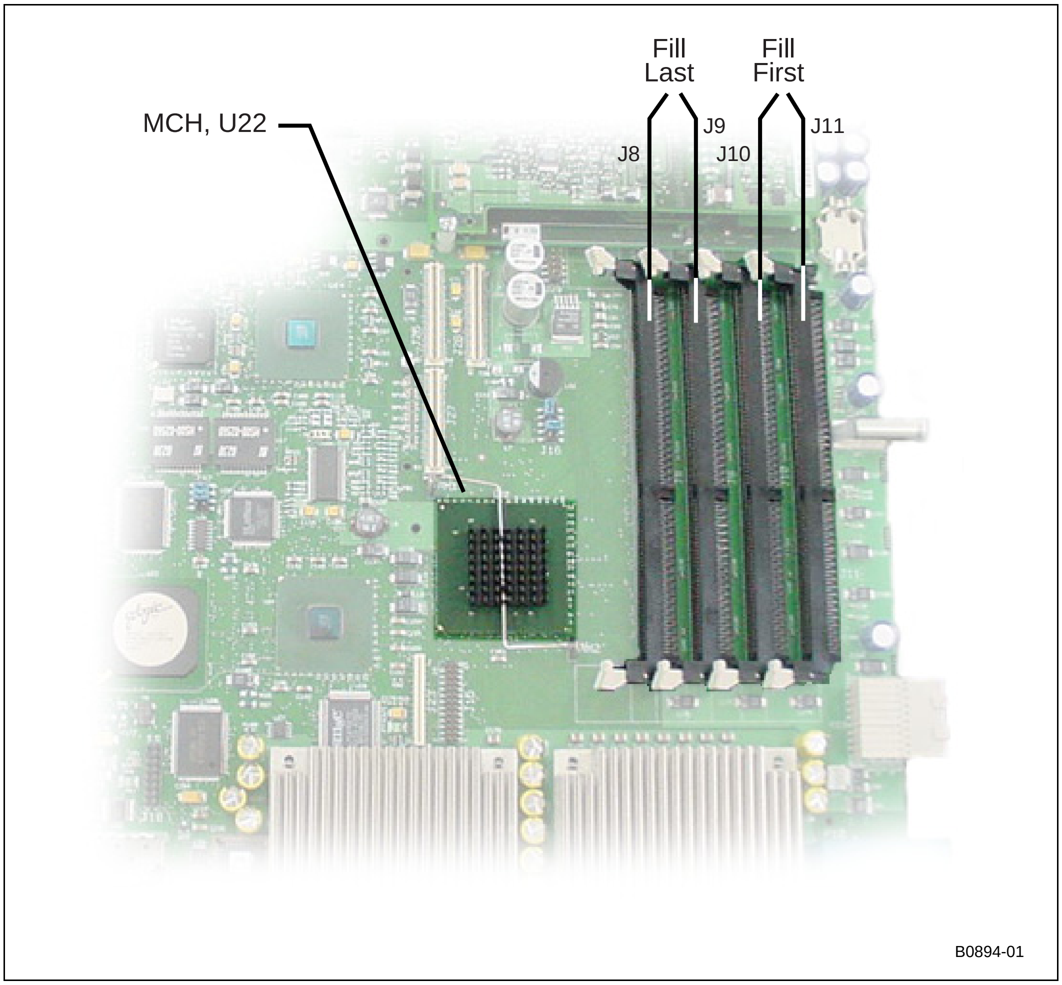
Four DDR 266 DIMM sockets make up the memory subsystem. See Figure 18, "Intel® NetStructure™ AT8000 Component Layout" on page 77 for their locations. The MCH defines two memory channels operating in parallel to logically create a 144-bit wide memory data path. ECC is generated and checked across 128 bits of data, allowing for significant improvement in error correction.

Due to this architecture, DDR DIMMs must be installed in matched pairs. Memory DIMM configurations ranging from 512 MBytes to 8 GBytes in 512 MByte increments are supported.

2.2.3.1 Memory Ordering Rule for the MCH

Platforms based on the E7501 chipset require DDR DIMMs to be populated in matched pairs in a specific order. Start with the two DIMMs furthest from the MCH in a "fill-farthest" approach (see Figure 2). This requirement is based on the signal integrity requirements of the DDR interface.

Figure 2. Memory Ordering



2.2.4 I/O

2.2.4.1 Super I/O (U28)

The Super I/O device (SIO) is an SMSC LPC47B272 enhanced Super I/O controller. The SIO connects to the ICH3 through its LPC bus connection. The SIO provides support for the front panel serial port (J17, see page 64). There is no front-panel connection to the legacy keyboard and mouse PS/2 ports. Keyboard and mouse support are provided by the USB connection (J12, see page 63). See Figure 11 for connector locations.

To facilitate debug and BIOS development, SIO connections such as legacy (PS/2) keyboard/mouse and floppy may be provided on initial board revisions. Software must not rely on the presence of these connections on future board revisions.

2.2.4.2 Real-Time Clock

The AT8000 SBC real-time clock is integrated into the ICH3. It is derived from a 32.768 KHz crystal with the following specifications:

- Frequency tolerance @ 25 °C: ±20ppm
- Frequency stability: maximum of -0.04ppm/(Ä°C)^2
- Aging ÄF/f (1st year @ 25 °C): ±3ppm
- ±20ppm from 0-55 °C and aging 1ppm/year

The real-time clock is powered by a 0.22F SuperCap* capacitor when main power is not applied to the board. This capacitor powers the real-time clock for a minimum of two hours while external power is removed from the AT8000 SBC.

See Section 3.10.7, "Watchdog Timers (WDTs)" on page 52 for information about the real-time clock timers.

2.2.4.3 Timer0 Capabilities

Timer0, integrated inside the ICH3, is an 8254 compatible timer. This timer is set up to generate a periodic waveform that creates the edge for the timer0 interrupt. The interrupt is received by the ICH3 APIC and communicated to the CPU(s).

AT8000 provides a high-precision 14.318 MHz crystal clock source as the reference for the timer0 counters. To improve timing accuracy, the crystal used is a low-PPM, high-stability component with the following specifications:

- Frequency tolerance (25° C): ±10ppm
- Temperature characteristics (-10° C to +60° C): ±5ppm
- Aging: ±1ppm per year max

This timer does not operate when board power is removed.

2.2.4.4 Gigabit Ethernet (U13)

The AT8000 SBC implements two Gigabit Ethernet interfaces, each of which is routed to the fabric/switch slot through the backplane (J23, see page 62). There are no direct, external Ethernet ports included on the SBC board. Each Ethernet connection utilizes an 82546 Dual Gigabit Ethernet Controller, allowing support for 1000Mbits/s, 100Mbits/s and 10Mbits/s data rates.

The 82546 controller is optimized for designs using the PCI and the emerging PCI-X bus interface extension. The AT8000 SBC has a 133 MHz PCI-X bus connection. The integrated physical layer circuitry (PHY) provides an IEEE 802.3 Ethernet Interface for 1000Base-T, 100Base-TX, and 10Base-T applications.

Features include:

- 32/64-bit 33/66 MHz, PCI Rev 2.2 compliant interface
- Host interface also compliant with the PCI-X addendum, Rev 1.0a, from 50 to 133 MHz
- Supports 64-bit addressing
- Efficient PCI bus master operation, supported by optimized internal DMA controller

- Supports advanced PCI commands such as MWI, MRM, and MRL, and PCI-X commands such as MRD, MRB, and MWB
- Full IEEE 802.3ab auto-negotiation of speed, duplex, and flow-control configuration
- Complete full duplex and half duplex support
- Automatic MDI crossover operation for 100Base-TX and 10Base-T modes
- Automatic polarity correction
- Digital implementation of adaptive equalizer and canceller for echo and crosstalk

2.2.4.5 Fibre Channel (U23) - Optional

The QLogic* ISP2312 dual Fibre Channel controller is used for access to high-speed storage subsystems. It is routed through backplane connector P23.

See Figure 18, “Intel® NetStructure™ AT8000 Component Layout” on page 77 for its location.

This controller supports PCI and PCI-X bus interfaces. Burst mode master DMA transfers are utilized for efficient usage of bus bandwidth during data transfers, and 8, 16, and 32-bit accesses are supported as a PCI target. The controller appears as two independent Fibre Channel ports. A PCI function is assigned to each port in the device’s PCI configuration space. Functions 0 and 1 are used to configure FC ports 1 and 2, respectively.

ISP2312 features include:

- 32/64-bit 33/66 MHz, PCI Rev 2.2 compliant interface.
- Host interface compliant with the PCI-X addendum, Rev 1.0a, from 50 to 133 MHz.
- Supports 64-bit addressing (addresses >32 bit initiate use of DAC address cycle).
- Efficient PCI bus master operation, supported by optimized internal DMA controller.
- Supports advanced PCI commands such as MWI, MRM, and MRL, and PCI-X commands such as MRD, MRB, and MWB.
- Automatically negotiates Fibre Channel bit rate 1.06 Gbits/s (through backplane or front panel) or 2.12 Gbits/s (through front-panel Fibre Channel ports only)
- Supports up to 533 MBytes sustained FC data transfer rate (combined bandwidth of both directions transmitting simultaneously).
- Supports Fibre Channel-arbitrated loop (FC-AL), FC-AL-2, point-to-point, and switched fabric topologies.
- Maxim MAX3840 2x2 crosspoint switch for switching Fibre Channel between the front ports and the backplane, either via the BIOS Setup Menu by electronic keying.
- Each FC port includes:
  - Internal RISC processor
  - Receive DMA sequencer
  - Frame buffer
  - DMA channels (transmit, receive, command, auto-request, and auto-response)

- Support for JTAG boundary scan.
- Supports IP as well as other protocols; however there are currently no plans to validate protocols other than SCSI_FCP.

Each Fibre Channel interface of the ISP2312 includes its own internal 16-bit RISC processor and external 7.5 ns synchronous SRAM memory for instruction code and data. Parity protection is provided on accesses to this memory. The SBC utilizes two 256 KByte (128Kx18) SRAMs, one for each port, for the ISP2312 memory requirements.

An external 256 x 16 non-volatile EEPROM is used to store system configuration parameters and PCI subsystem and subsystem vendor IDs. The first 128 bytes are used for function 0 parameters and the second 128 bytes are used for function 1.

2.2.5 PMC Connector (J25, J26, J27)

The AT8000 SBC supports one 64-bit, 66 MHz PMC slot. The PMC slot is connected to the second of two P64H2 hub controllers via PMC Connectors J25-J27. The PMC slot has an opening in the front panel of the SBC that exposes the I/O connectors of the add-in PMC card. PMC cards can only be added to or removed from this slot when the board is outside the system chassis. See Figure 18, “Intel® NetStructure™ AT8000 Component Layout” on page 77 for its location.

The PCI bus specification provides the means for backward compatibility with slower PMC cards (32-bit or 33 MHz) through the use of the M66EN pin. A PMC card that does not support 66 MHz operation grounds the M66EN pin when installed to inform the SBC hardware to provide a 33 MHz clock to this interface. Support for 32-bit only PMC cards is accomplished through the use of the REQ64#/ACK64# PCI bus protocol.

The PMC slot provided by the SBC connects the PCI VI/O voltage pins to +3.3 V. This requires use of PMC plug-in cards that support +3.3 V I/O signal levels. Only PMC plug-in cards designated “+3.3 V only” or “universal” voltage I/O are supported. The PMC plug-in location provides a key pin to prevent insertion of cards that do not meet this requirement. Note that +5 V power is still supplied to the PMC pins designated for +5 V connections. The PMC is allotted 1.5 A of current.

2.2.6 Firmware Hub (U30, U33)

The AT8000 SBC supports two 8Mbit (1 MByte) BIOS flash ROMs:

- Primary BIOS flash ROM (FWH0)
- Recovery BIOS flash ROM (FWH1)

The flash is allocated for BIOS and Firmware usage.

The SBC boots from the primary flash ROM under normal circumstances. During the boot process, if the BIOS (or IPMC) determines that the contents of the primary flash ROM are corrupted, a hardware mechanism is available to change the flash device select logic to the recovery flash ROM. See Section 2.2.6.1, “Flash ROM Backup Mechanism” on page 23 for more information.

Each flash component has a separately write-protected boot block that prevents erasure when the device is upgraded.

Flash ROM BIOS updates can be performed by an end user or a network administrator over the LAN. The system should complete booting to an OS, MS-DOS* or logon to Linux* as root user. The system should have a local copy of the flash program and the BIOS data files or have the capability to copy the flash program and BIOS data files onto a local drive via the network. The flash program has a command line interface to specify the path and the file name of the BIOS data files. After completing the BIOS ROM update the user should shutdown and reset the system to let the new BIOS ROM take effect. See Section 7.7, “BIOS Updates” on page 89 for more information.

2.2.6.1 Flash ROM Backup Mechanism

The on-board Intelligent Platform Management Controller (IPMC) manages which of the two BIOS flash ROMs is used during the boot process. The IPMC monitors the boot progress and can change the flash ROM selection and reset the processor.

The default state of this control configures the primary Firmware Hub (FWH) ROM device ID to be the boot device; the secondary FWH is assigned the next ID. The secondary FWH responds to the address range just below the primary FWH ROM in high memory.

The Intelligent Platform Management Controller sets the ID for both FWH devices. Boot accesses are directed to the FWH with ID = 0; unconnected ID pins are pulled low by the FWH device. In this way the IPMC may select which flash ROM is used for the boot process.

Refer to Section 3.7.1, “Reset BIOS Flash Type” on page 39 for a description of how to do this manually.

2.2.7 Onboard Power Supplies

The main power supply rails on the AT8000 SBC are powered from dual-redundant -48 V power supply inputs from the backplane power connector (P10). There are also dual redundant, limited current, make-last-break-first (MLBF) power connections. See Figure 18, “Intel® NetStructure™ AT8000 Component Layout” on page 77 for their location.

2.2.7.1 Power Feed Fuses

As required by the PICMG* 3.0 specification, the AT8000 SBC provides fuses on each of the -48V power feeds and on the the RTN connections as well. The fuses on the return feeds are critical to prevent overcurrent situations if an ORing diode in the return path fails and there is a voltage potential difference between the A and B return paths.

2.2.7.2 ORing Diodes and Circuit Breaker Protection

The two -48 V power connectors are OR’d together. A current limiting FET switch is connected between the OR’d -48 V and the primary DC-DC converters. The FET switch provides three functions:

- A mechanism to electrically connect/disconnect the SBC to/from the two -48 V inputs.
- A soft-on function.
- An over-current circuit breaker feature.

2.2.7.3 -48 V to +12 V Converter

This converter provides DC isolation between the -48 V and -48 V return connections and all of the derived DC power on the AT8000 SBC. Its output is connected to the SBC’s +12 V power rail. The converter supplies a maximum of 9 A of current. The converter is enabled/disabled by the onboard IPMC.

2.2.7.4 -48 V to +5 V/+3.3 V Converter

This converter provides DC isolation between the -48 V and -48 V return connections and all of the derived DC power on the AT8000 SBC. Its output is connected to the SBC's +5 V and 3.3 V power rails. The converter supplies a maximum of 9 A of +5 V current and 9 A of +3.3 V current. The converter is enabled/disabled by the onboard IPMC.

2.2.7.5 Processor Voltage Regulator Module (VRM)

The Voltage Regulator Module (VRM) provides core power to the two Low Voltage Xeon processors. The input to the VRM is connected to the +12 V power rail.

See Figure 18, "Intel® NetStructure™ AT8000 Component Layout" on page 77 for its location.

The VRM controller is designed to support multiple processor core voltages selected by the voltage identification (VID) pins on the processor. Logic provided on the SBC ensures that the VRM is not enabled if the two processors request different VID codes. In addition, the VRM is disabled until all other voltage converters indicate "power good." The voltage regulator module is designed to support up to two 43 W (TDP - Thermal Design Power) processors.

Note: The +5 VSB power rail only needs to supply at least 4.0 V to properly power any circuitry that uses the +5 VSB rail when the payload power (i.e., processors, ethernet controller, etc.) is not turned on. Any alerts from the +5 VSB sensor when the system is not in the M4, M5, or M6 states should be ignored.

2.2.7.6 IPMB Standby Power

This converter provides DC isolation between the -48 V and -48 V return connections and all of the derived DC power on the AT8000. Its output is connected to the IPMB and standby +5 V power rail of the SBC. The converter supplies a maximum of 1.5 A of +5 V current. A +3.3 V management voltage is derived from the IPMB power by means of a linear regulator circuit and is used to power most of the IPMC functions. Standby power is derived from the -48 V rails and is always available on the SBC unless the overall system power rail (-48 V) is shut down.

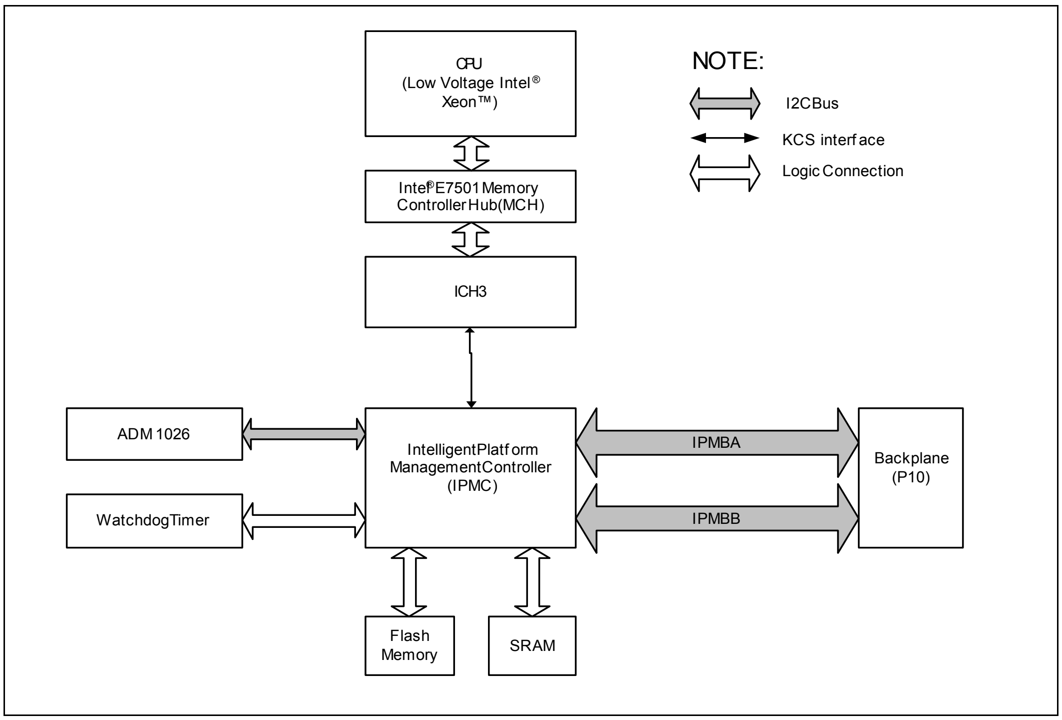
![kontron ... always a Jump ahead!]

Hardware Management Overview 3

The Intelligent Platform Management Controller (IPMC) is an Intel-designed baseboard management controller device manufactured by Philips Semiconductor* for Intel.

The high-level architecture of the baseboard management for AT8000 is represented in the block diagram below.

Figure 3. Hardware Management Block Diagram



The main processors communicate with the IPMC using the Keyboard Controller Style (KCS) interface. Two KCS interfaces are available for the BIOS to communicate to the IPMC. BIOS uses SMS interface for normal communication and SMM interface when executing code under systems management mode (SMM). The base address of the LPC interface for SMS is 0xCA2 and 0xCA4 for SMM operation. Besides that, the BIOS is able to communicate with the IPMC for POST error logging purposes, fault resilient purposes, and critical interrupts via the KCS interface.

The memory subsystem of the IPMC consists of a flash memory to hold the IPMC operation code, firmware update code, system event log (SEL), and a sensor data record (SDR) repository. RAM is used for data and occasionally as a storage area for code when flash programming is under execution. The field replacement unit (FRU) inventory information is stored in the nonvolatile memory on ADM1026. The flash memory can store up to 64 KBytes of SEL events and SDR information, while the ADM1026 can store up to 512 bytes of FRU information. Having the SEL and logging functions managed by the IPMC helps ensure that 'post-mortem' logging information is available even if the system processor becomes disabled.

The IPMC provides six I2C bus connections. Two are used as the redundant IPMB bus connections to the backplane while another one is used for communication with the ADM1026. The remaining buses are unused. If an IPMB bus fault or IPMC failure occurs, IPMB isolators are used to switch and isolate the backplane/system IPMB bus from the faulted SBC board. Where possible, the IPMC activates the redundant IPMB bus to re-establish system management communication to report the fault.

The onboard DC voltages are monitored by the ADM1026 device, manufactured by Analog Devices. The IPMC queries the ADM1026 over a local system management I2C bus. The ADM1026 includes voltage threshold settings that can be configured to generate an interrupt to the IPMC if any of the thresholds are exceeded.

To increase the reliability of the AT8000 SBC, a watchdog timer is implemented, whereby it strobes an external watchdog timer at two-second intervals to ensure continuity of operation of the board's management subsystem. If the IPMC ceases to strobe the watchdog timer, the watchdog timer isolates the IPMC from the IPMBs and resets the IPMC. The watchdog timer expires after six seconds if strobes are not generated, and it resets the IPMC. Detailed information on the watchdog timer configuration can be queried using standard IPMI v1.5 watchdog timer commands. The watchdog timer does not reset the payload power.

3.1 Sensor Data Record (SDR)

Sensor Data Records contain information about the type and number of sensors in the baseboard, sensor threshold support, event generation capabilities, and the types of sensor readings handled by system management firmware.

The AT8000 management controller is set up as a satellite management controller (SMC). It does support sensor devices, whose population is static by nature. SDRs can be queried using Device SDR commands to the firmware. Refer to Section B, "List of Supported Commands (IPMI v1.5 and PICMG 3.0)" on page 141 for the list of supported IPMI commands for SDRs. Hardware sensors that have been implemented are listed below.

Table 2. Hardware Sensors

Sensor Number	Sensor Type	Voltage/Signals Monitored	Monitored via	Scanning Enabled under Power State	Health LED (Green to Red)
1Dh	Voltage	+1.5 V	ADM 1026	Power On	Exceeds critical threshold
17h		+2.5 V	ADM 1026	Power On	Exceeds critical threshold
16h		+1.8 V	ADM 1026	Power On	Exceeds critical threshold
15h		VTT DDR (+1.25 V)	ADM 1026	Power On	Exceeds critical threshold
14h		+1.2 V	ADM 1026	Power On	Exceeds critical threshold
19h		+5 V	ADM 1026	Power On	Exceeds critical threshold
1Bh		-12 V	ADM 1026	Power On	Exceeds critical threshold
1Ah		+12 V	ADM 1026	Power On	Exceeds critical threshold
1Ch		CPU Core Voltage	ADM 1026	Power On	Exceeds critical threshold
18h		+3.3 V	ADM 1026	Power On	Exceeds critical threshold
12h		+1.8 VSB	ADM 1026	Power On/Off	Exceeds critical threshold
11h		+5 VSB	ADM 1026	Power On/Off	Exceeds critical threshold
13h		V BAT	ADM 1026	Power On/Off	Exceeds critical threshold
30h	Temperature	Board Temperature	ADM 1026	Power On/Off	Exceeds critical threshold
37h		CPU 0 Temperature	ADM 1026	Power On	Exceeds critical threshold
38h		CPU 1 Temperature	ADM 1026	Power On	Exceeds critical threshold
50h	Processor	CPU 0 Presence	ADM 1026	Power On/Off	No change
50h		CPU 0 IERR	IPMC	Power On	No change
50h		CPU 0 Thermtrip	IPMC	Power On	ThermTrip signal asserted
56h		CPU 0 ProcHot	IPMC	Power On	ProcHot signal asserted
51h		CPU 1 Presence	ADM 1026	Power On/Off	No change
51h		CPU 1 IERR	IPMC	Power On	No change
51h		CPU 1 Thermtrip	IPMC	Power On	ThermTrip signal asserted
57h		CPU1 ProcHot	IPMC	Power On	ProcHot signal asserted
8Ah	FRU Hot Swap	FRU State	IPMC	Power On/Off	No change
8Bh	IPMB Link Sensor	Operational state of IPMB-0	Logical	Power On/Off	No change
07h	CPU Critical Interrupt	PCI SERR	IPMC	Power On	No change
		PCI PERR	IPMC	Power On	No change
06h	System Firmware Progress		IPMC	Power On	No change
08h	Memory Error	ECC Multiple Bit error	IPMC	Power On	No change
		ECC Single Bit error	IPMC	Power On	No change
03h	Watchdog Timer	IPMC Watchdog Timer timeout	IPMC	Power On/Off	No change
54h	Boot Error	BIOS Main Flash	IPMC	Power On	No change
55h		BIOS FRED Flash	IPMC	Power On	No change
83h	System Event	System Event	IPMC	Power On	No change

3.2 System Event Log (SEL)

The SEL is the collection of events that are generated by the IPMC. vent logs are stored in non-volatile memory. This resides on the board and allows better tracking of error conditions on the baseboard when it is moved from chassis to chassis. Having the SEL and logging functions managed by the IPMC helps ensure that post-mortem logging information is available should a failure occur that disables the systems processor(s). In the AT8000, flash memory for IPMI firmware can store up to 3276 SEL entries. Management software running on the host processor is responsible for ensuring that SEL storage has sufficient space for SEL logging. Events are normally forwarded to shelf manager and logged to SEL on the board. If SEL storage on the board is full, new events are forwarded to the Shelf Manager but are not logged in to SEL on the board.

A set of IPMI commands (see Table 88, "IPMI 1.5 Supported Commands" on page 141) allows the SEL to be read and cleared and allows events to be added to the SEL. The IPMI commands used for adding events to the SEL are *Platform Event Message, Add SEL entry,* and *Partial Add Entry*. Table 3, "SEL Events Supported by the AT8000" on page 28 lists supported SEL events. Event Messages can be sent to the IPMC via the IPMB. This provides the mechanism for satellite controllers to detect events and log them into the SEL.

Table 3. SEL Events Supported by the AT8000 (Sheet 1 of 3)

Sensor Type	Sensor Type Code	Sensor-Specific Offset (Event Data 1, Bit 0-3)	Event	Remarks
Reserved	00h	-	Reserved	-
Temperature	01h	-	Temperature	Threshold exceeded for upper critical, upper non-critical, lower critical and lower non-critical thresholds. Refer to Table 4, "Sensor Thresholds for IPMC Firmware 1.0" on page 31 for sensor thresholds data.
Voltage	02h	-	Voltage	Voltage exceeded upper critical, upper non-critical, lower critical and lower non-critical thresholds. Refer to Table 4 for sensor thresholds data.
Processor	07h	00h	IERR	Processor IERR has occurred.
		01h	Thermal Trip	Processor thermal trip has occurred.
		07h	Processor Presence detected	
		09h	Terminator Presence Detected	
Memory	0Ch	00h	Correctable ECC	Event data 3 = DIMM pair number
		01h	Uncorrectable ECC	Event data 3 = DIMM pair number
System Firmware Progress	0Fh	00h	Timer Count Read/ Write error	Event data 2 = FEh Event data 3 = 00h
			CMOS Battery error	Event data 2 = FEh Event data 3 = 01h
			CMOS Diagnosis status error	Event data 2 = FEh Event data 3 = 02h
			CMOS Checksum error	Event data 2 = FEh Event data 3 = 03h
			CMOS Memory Size error	Event data 2 = FEh Event data 3 = 04h

Table 3. SEL Events Supported by the AT8000 (Sheet 2 of 3)

Sensor Type	Sensor Type Code	Sensor-Specific Offset (Event Data 1, Bit 0-3)	Event	Remarks
System Firmware Progress, continued	0Fh	00h	RAM Read/Write test error	Event data 2 = FEh Event data 3 = 05h
			CMOS Date/Time error	Event data 2 = FEh Event data 3 = 06h
			Clear CMOS jumper	Event data 2 = FEh Event data 3 = 07h
			Clear Password Jumper	Event data 2 = FEh Event data 3 = 08h
			Manufacturing Jumper	Event data 2 = FEh Event data 3 = 09h
			BMC in update error	Event data 2 = FEh Event data 3 = 0Ah
			BMC Response Fail error	Event data 2 = FEh Event data 3 = 0Bh
			Event Log Full error	Event data 2 = FEh Event data 3 = 0Ch
Event Logging Disabled	10h	00h	Correctable Memory Error Logging Disabled	Error Logging will be disabled after 10 events within one hour.
Critical Interrupt	13h	04h	PCI PERR	Event data 2 = Bus No. Event data 3 =Device/Func No.
		05h	PCI SERR	Event data 2 = Bus No. Event data 3 =Device/Func No.
		07h	PCI Non-Fatal error	Event data 2 = Bus No. Event data 3 =Device/Func No.
System ACPI Power state	22h	00h	S0/G0	Board is running
		06h	S4/S5	Soft-off
		0Bh	Legacy ON state	Indicate ON for board that doesn't support ACPI
		0Ch	Legacy OFF state	Legacy soft-off
Watchdog	23h	00h	Timer expired, status only	
		01h	Hard Reset	POST/Boot monitor timed out
		02h	Power Down	OS WDT shutdown after the monitor timeout
		03h	Power Cycle	OS WDT reset after the monitor timeout
IPMB Link Sensor	F1h	00h	IPMB A & B disabled	Refer PICMG 3.0 Specifications (Table 3-46)
		01h	IPBM A enabled IPMB B disabled	
		02h	IPMB A disabled IPMB B disabled	
		03h	IPMB A & B enabled	

Table 3. SEL Events Supported by the AT8000 (Sheet 3 of 3)

Sensor Type	Sensor Type Code	Sensor-Specific Offset (Event Data 1, Bit 0-3)	Event	Remarks
FRU Hot swap	F0h	07h	M7 - FRU inactive	Refer to PICMG 3.0 Specifications (Table 3-14)
		06h	M6 - FRU activation request	
		05h	M5 - FRU activation in progress	
		04h	M4 - FRU active	
		03h	M3 - FRU deactivation request	
		02h	M2 – FRU deactivation in progress	
		01h	M1 – Communication lost	
		00h	M0 – FRU not installed	

3.2.1 Temperature and Voltage Sensors

Temperature and voltage readings are monitored by ADM1026. They are critical sensors that ensure the AT8000 is operating at its predefined threshold limits. The sensors are categorized as follows:

- Lower Non-Critical
- Lower Critical
- Upper Non-Critical
- Upper Critical

If the lower critical or upper critical threshold is exceeded, it raises a major alarm. If the lower non-critical or upper non-critical threshold is exceeded, it raises a minor alarm.

Only critical thresholds which are exceeded turn on the solid red LED. However, for any events above, IPMC forwards the events to the shelf manager to log it into shelf manager's SEL.

Table 4. Sensor Thresholds for IPMC Firmware 1.0

Sensor Name	Sensor Number	System Event Log, reported via CLI, SNMP, RPC, RMCP	Normal Value	LNR	LC	LNC	UNC	UC	UNR
+1.5 V	1Dh	Yes	+1.5 V	TBD	1.43	1.45	1.55	1.57	–
+2.5 V	17h	Yes	+2.5 V	TBD	2.3	2.36	2.625	2.7	–
+1.8 V	16h	Yes	+1.8 V	TBD	1.71	1.746	1.854	1.89	–
VTT DDR (+1.25 V)	15h	Yes	+1.25 V	TBD	1.185	1.20	1.3	1.315	–
+1.2 V	14h	Yes	+1.2 V	TBD	1.14	1.176	1.224	1.26	–
+5 V	19h	Yes	+5 V	TBD	4.7	4.85	5.25	5.275	–
-12 V	1Bh	Yes	-12 V	TBD	-13.2	-12.6	-11.4	-10.8	–
+12 V	1Ah	Yes	+12 V	TBD	10.8	11.4	12.6	13.2	–
CPU Core Voltage	1Ch	Yes	+1.3 V	TBD	1.24	1.26	1.345	1.36	–
+3.3 V	18h	Yes	+3.3 V	TBD	3.102	3.201	3.465	3.482	–
+1.8 VSB	12h	Yes	+1.8 V	TBD	1.71	1.73	1.836	1.89	–
+3.3 VSB	10h	Yes	+3.3V	TBD	3.102	3.201	3.465	3.482	–
+5 VSB	11h	Yes	+5 V	TBD	4.09	4.19	5.25	5.275	–
VBAT	13h	Yes	+3 V	TBD	2.0	2.4	3.4	3.6	–
Board Temperature	30h	Yes	30	TBD	-5	5	60	70	–
CPU 0 Temperature	37h	Yes	40	TBD	5	10	76	81	–
CPU 1 Temperature	38h	Yes	40	TBD	5	10	76	81	–

NOTE: The following terms apply:
LNR: Lower Non-Recoverable
LC: Lower Critical
LNC: Lower Non-Critical
UNC: Upper Non-Critical
UC: Upper Critical
UNR: Upper Non-critical

Table 5. Sensor Thresholds for IPMC Firmware 1.2

Sensor Name	Description	Sensor Number	Normal Value	Thresholds				
				Lower Critical	Lower Noncritical	Upper Noncritical	Upper Critical	Upper Non-recoverable
+1.5V	+1.5V	1Dh	1.5	1.43 (1.45)	-	-	1.57 (1.54)	
+2.5V	+2.5V	17h	2.49	2.29 (2.32)	2.35 (2.375)	2.63 (2.609)	2.69 (2.67)	-
+1.8V	+1.8V	16h	1.79	1.71 (1.73)	-	-	1.88 (1.86)	-
VTT DDR	DDR Voltage	15h	1.24	1.19 (1.16)	-	-	1.31 (1.29)	-
+1.2V	+1.2V	14h	1.2	1.14 (1.16)	-	-	1.25 (1.24)	-
+5V	+5V	19h	4.99	4.73 (4.78)	-	-	5.23 (5.17)	-
-12V	-12V	1Bh	-12.11	-15.06 (-14.92)	-12.83 (-12.69)	-11.25 (-11.39)	-7.5 (-7.65)	-
+12V	+12V	1Ah	12.1	7.56 (7.63)	11.28 (11.313)	12.85 (12.63)	15.06 (14.88)	-
CPU Core Voltage	CPU Core Voltage	1Ch	1.31	1.24 (1.25)	-	-	1.37 (1.33)	-
+3.3V	+3.3V	18h	3.3	3.13 (3.17)	-	-	3.46 (3.41)	-
+1.8VSB	+1.8V on standby rail	12h	1.79	1.71 (1.73)	-	-	1.88 (1.86)	-
+3.3VSB	+3.3V on standby rail	10h	3.3	3.13 (3.17)	-	-	3.46 (3.41)	-
+5VSB	+5V on Standby rail	11h	5	4.09 (4.14)	-	-	5.24 (5.19)	-
VBAT	Battery voltage	13h	3.55	1.99 (2.03)	3.31 (3.35)	-	-	-
Baseboard Temp	Board temperature	30h	30	-5 (-2)	5 (8)	60 (57)	70 (67)	80 (77)
CPU 1 Temp	CPU 1 (Right) temperature	37h	40	5 (8)	10 (13)	76 (73)	81 (78)	127 (124)
CPU 2 Temp	CPU 1 (Left) Temperature	38h	40	5 (8)	10 (13)	76 (73)	81 (78)	127 (124)

NOTE: The value in parentheses is the deassertion value.

3.2.2 Processor Events

The processor asserts IERR as the result of an internal error. A thermal trip error indicates the processor junction temperature has reached a level where permanent silicon damage may occur. Upon THERMTRIP assertion, the IPMC powers down the boards.

3.2.3 DIMM Memory Events

The MCH (E7501) instructs the ICH3 to report memory parity errors via SMI#. The SMI handler extracts the error information (address) from the DRAM error registers in the MCH and logs it into the SEL. The KCS interface performs error reporting to IPMC. BIOS sends a platform event message with the appropriate data to the IPMC, which logs the event to SEL and forwards the event to the Shelf Manager. Correctable memory errors generate an SMI and are logged into SEL. Normally, a board with non-correctable errors is likely to hang as the multi-bit error may cause the CPU to execute corrupted instructions. If the CPU executes corrupted instructions before executing the code to log the event, then this event will not be logged in the SEL.

3.2.4 System Firmware Progress (POST Error)

The BIOS is able to log both POST and critical events to the IPMC error log. (Refer to Table 51, "BIOS Error Messages" on page 93.)

3.2.5 Critical Interrupts

In general, the system BIOS is capable of generating requests on the KCS interface to communicate with the IPMC for error logging, fault resilience, critical interrupts and reading/writing inventory CPUs and RAM information to the IPMC. Two LPC interfaces are available for the BIOS to communicate to the IPMC. The BIOS uses the SMS interface for normal communication with the IPMC and the SMM interface when executing code under SMM mode.

PCI errors implemented in the AT8000 are handled as follows:

1. The MCH(E7501) sends a parity error/system error (PERR/SERR) message over the hub interface to the ICH3 notifying it that an error occurred.
2. The ICH3 generates an SMI# interrupt when it receives a PERR/SERR message.
3. The SMI handler checks the error status registers of CPU/MCH until it identifies the source and type of the error.
4. The handler sends a message to the IPMC via the KCS interface, causing it to log the error in the IPMC's event log. IPMC then forwards the event to Shelf Manager to log it into Shelf Manager SEL.

3.2.6 System ACPI Power State

AT8000 is targeted to support ACPI functionality, with support for the sleep states S0, S4 & S5. On assertion of ICH3_SLP_S5# and ICH3_SLP_S3# GPIOs, IPMC sends out a hot-swap event message to the shelf manager requesting deactivation. On successful reception of a deactivation message from the shelf manager, the FRU enters M1 power state and remains in this state.

Under conditions where an ACPI enabled operating system is in S4/S5 sleep state, the chipset could deassert ICH3_SLP_S5# and ICH3_SLP_S3# GPIOs requiring the IPMC to attempt ATCA power state transition to M4 state (through M2, M3).

ACPI capabilities of an operating system are communicated by BIOS to the IPMC at initialization. An OEM style IPMI command is sent by BIOS for this purpose. This command (*SetACPIConfig* ; *NetFn: 30h, command: 83h*) is sent by BIOS every time an operating system is initialized. The IPMC firmware defaults to no ACPI until this command is received with proper data in the request to indicate the OS is either ACPI enabled or disabled. For obvious reasons, this command is only executable over SMS channel.

3.2.7 IPMB Link Sensor

The AT8000 provides two IPMB links to increase communication reliability to the shelf manager and other IPM devices on the IPMB bus. These IPMB links work together for increased throughput where both busses are actively used for communication at any point. A request might be received over IPMB Bus A, and the response is sent over IPMB Bus B. Any requests that time out are retried on the redundant IPMB bus. In the event of any link state changes, the events are written to the AT8000 SEL. IPMC monitors the bus for any link failure and isolates itself from the bus if it detects that it is causing errors on the bus. Events are sent to signify the failure of a bus or, conversely, the recovery of a bus.

3.2.8 FRU Hot Swap

The hot-swap event message conveys the current state of the FRU, the previous state, and a cause of the state change as can be determined by the IPMC. Refer to PICMG 3.0 Specifications for further details on the hot-swap state.

3.3 Field Replaceable Unit (FRU) Information

The FRU Information provides inventory data about the boards where the FRU Information Device is located. The part number or version number can be read through software.

FRU information in the AT8000 includes data describing the AT8000 board as per PICMG 3.0 specification requirements. Additional multirecords will be added for the BIOS to write CPU information, BIOS version number, and PMC information to FRU data correctly. This information is retrieved by shelf manager (ShMC), enabling reporting of board-specific information through an out-of-band mechanism.

Following are the definitions for the multirecord implemented by the firmware as part of FRU data.

Table 6. FRU Multirecord Data for CPU/RAM/PMC/BIOS Version Information (Sheet 1 of 2)

Variable	Size (byte)	Data	Type
Manufacturer ID (Intel IANA number)	3	0x000157 (LSB first, MSB next)	Binary
Record Version	1	1	Binary
Type/Length	1	1	Binary
CPU No.s	1	x	Binary
Type/Length	1	2	Binary
RAM Info	2	X (in units of 1 MByte)	Binary
Type/Length	1	(4 * XXX) + 1	Binary
No. of PMCs	1	XXX	Binary
PMC Info	4*XXX	PMC_Data	Binary

Table 6. **FRU Multirecord Data for CPU/RAM/PMC/BIOS Version Information (Sheet 2 of 2)**

Variable	Size (byte)	Data	Type
Type/Length	1	0xFF	Binary
BIOS Version	63 (max)	yyyyyyyy	ASC-II
End of fields	1	0xC1	Binary

Table 7. **PMC Data**

Variable	Size	Data	Type
Device ID	2	XX	Binary
Vendor ID	2	XX	Binary

3.4 E-Keying

E-Keying has been defined in the PICMG 3.0 Specification to prevent board damage, prevent misoperation, and verify fabric compatibility. The FRU data contains the board point-to-point connectivity record as described in Section 3.7.2.3 of the PICMG 3.0 specification.

Upon management power-on, the firmware sets the Fibre Channel ports to front panel by default. When the board enters M3 power state, the shelf manager reads in the board point-to-point connectivity record from FRU and determines whether the board can enable the Fibre Channel ports to the back plane. Set/Get Port State IPMI commands defined by the PICMG 3.0 specification are used for either granting or rejecting the E-keys.

If user Fibre Channel selection is to the front, the firmware maintains the Fibre Channel ports to the front panel regardless of the shelf manager's granting or rejecting of E-keys for the board.

Table 8, "Link Descriptors for E-Keying" on page 35, describes the:

- Connections to base and fabric interfaces on the AT8000 board for E-keying purposes.
- Link descriptor list for the two Gigabit Ethernet channels connected to the base interface and the two Fibre Channels on the fabric interface.

Table 8. **Link Descriptors for E-Keying**

No	Link Descriptor	Link Grouping ID	Link Type Extension	Link Type	Link Designator			Link Desc Value
					Port 0 - 3 Flags	Interface	Channel Number	
		[31:24]	[23:20]	[19:12]	{11:8}	{7:6}	[5:0}	
1	Ethernet Port 1	0	0000	00000001	0001	00	000001	0x00001101
2	Ethernet Port 2	0	0000	00000001	0001	00	000010	0x00001102
3	FC Port 1	0	0010	00000010	1100	01	000001	0x00202C41
4	FC Port 2	0	0010	00000010	1100	01	000010	0x00202C42

NOTE: Fibre Channel E-keying is only applicable to AT8000FXX products.

3.5 IPMC Firmware Code

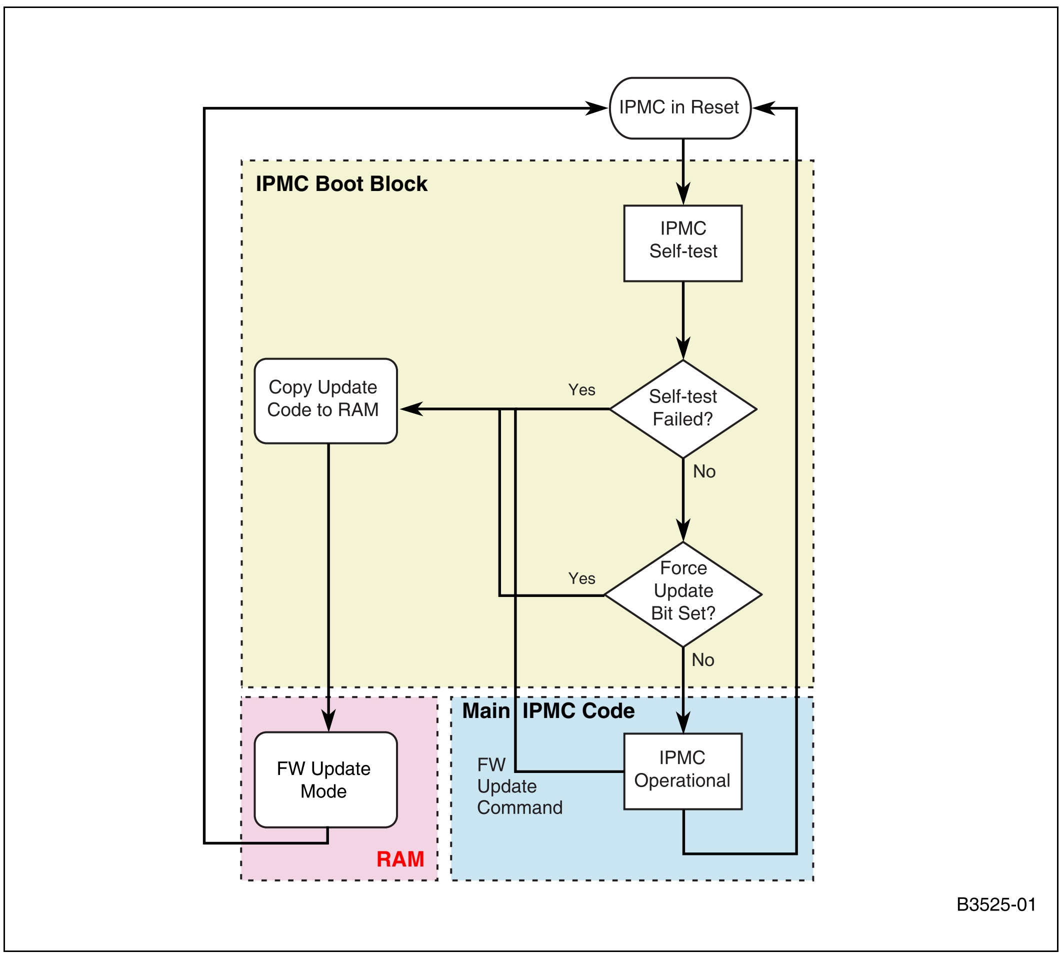
IPMC firmware code is organized into boot code and operational code, both of which are stored in a flash module. Upon an IPMC reset, the IPMC executes the boot code and performs the following:

1. Self test to verify the status of its hardware and memory.
2. Sets up the internal real-time operating system (RTOS).
3. Performs a checksum of the operational code.

Upon successful verification of the operational code checksum, the firmware will jump to the operational code.

When the firmware is commanded to enter firmware (FW) update mode, the operational code uses a special branch, Software Interrupt, to jump to the FW update code in the boot block. Once in FW update mode, the update code is copied into RAM, then the FW jumps to the code in RAM to execute. The FW update code cannot execute out of flash while the flash is being updated.

Figure 4. IPMC Firmware Code Process



3.6 IPMC Firmware Upgrade Procedure

AT8000 firmware is upgraded using either of two methods, the KCS interface or the IPMB (RMCP) interface.

3.6.1 IPMC Firmware Upgrade Using KCS Interface

The KCS interface is the communication mechanism between the host processor on the AT8000 and the IPMC controller. A firmware update utility is available. It takes a hex file to be updated as input from the command line. It can also verify that updates are completed successfully by reading back data written to the flash memory. Typically, it takes the utility around two minutes to complete the update over the KCS interface. After the firmware update is completed, the controller goes through a reset and boots up with the new firmware. The host processor is not reset when going through a firmware update, so the operating system and applications running on the host processor are not interrupted.

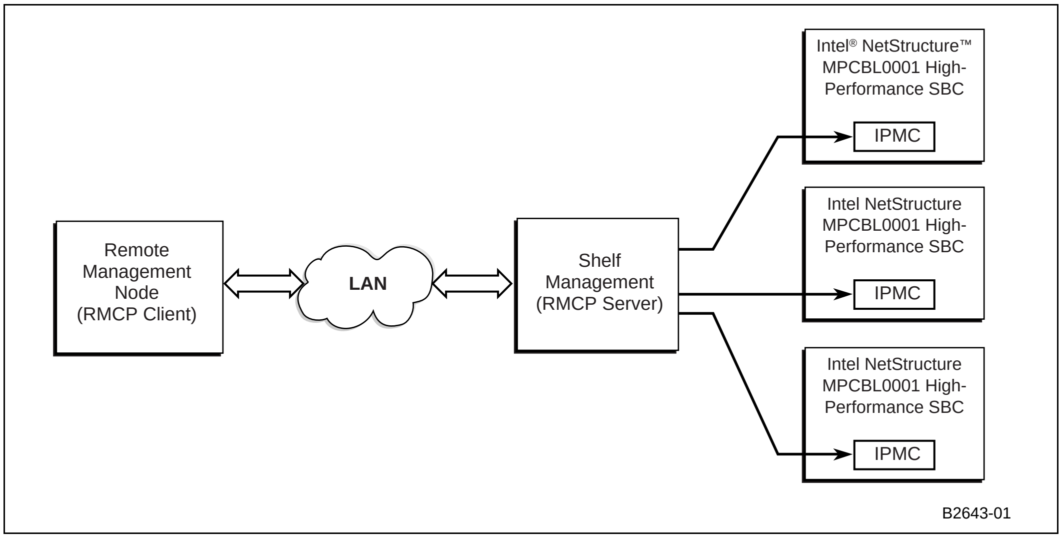
Below is a step-by-step procedure on how to update the firmware:

1. Copy the FW upgrade utility and FW upgrade (Hex) file to a DOS bootable floppy disk.
2. Boot AT8000 from a USB floppy disk (connected to the USB port) to a DOS prompt.
3. Copy the automatically generated (C: drive) Upgrade utility and hex file to RAM disk.
4. Issue the command “FWPIAUPD filename.hex” (or whatever the actual hex file name is).
5. AT8000 is now in FW upgrade mode. Select 'U' for updating firmware or 'V' to verify the hex image on the board with the image being used by the update utility.
6. The utility shows the versions on the board and on the hex image being updated.
7. Select 'Y' to update; follow the prompts and answer appropriately.

The upgrade ends with a message of successful termination.

3.6.2 IPMC Firmware Upgrade via the IPMB Interface (RMCP)

Figure 5. Upgrade via Remote Management Node



IPMI Specification v1.5 defines Remote Management Control Protocol (RMCP). Version 1.5 adds features for layering commands through virtual networks like Ethernet.

The IPMC firmware that needs to be upgraded is loaded to client utility software on the RMCP client. The RMCP client uses the RMCP protocol carrying embedded IPMI messages to send to the RMCP Server running in the CMM. The RMCP server decodes the RMCP package and forwards the IPMI messages to the SBC.

3.6.2.1 Updating AT8000 Firmware

To update the AT8000 firmware for the Intel® NetStructure™ AT8000 High- Performance Single Board Computer, execute the following commands.

1. Copy the update utility (fwpiaupd) and the firmware image file into the same directory in the RedHat Linux host. Note: If using ftp for file transfer, use binary mode to transfer files. The firmware image file or the utility file may get corrupted if binary mode is not used.
2. /fwpiaupd -ip [IPAddress] -user root -pwd cmmrootpass -ni -b -u -slot [slot#] filename.hex.

Note: The dot before / character in the command is required.

- IPAddress is the IP address of the CMM.
- At default, user is root. Password is cmmrootpass.
- slot# is slot 1 to 14 in the MPCHC0001 chassis.
- filename.hex is the firmware file.

Note: This "fwpiaupd" utility can only be supported on the Red Hat* Linux* 8.0 Platform. The Intel® NetStructure™ MPCMM0001 is needed for this remote update to work.

The utility and upgraded firmware are part of the IPMC Firmware release package. It can be downloaded from the Intel web site at http://www.intel.com/design/network/products/cbp/atca/index.htm.

3.7 OEM IPMI Commands

This section documents the OEM style IPMI commands implemented and supported on the AT8000.

3.7.1 Reset BIOS Flash Type

This command resets the processor and changes the BIOS bank select signal so that CPU boots off redundant BIOS bank.

Table 9. Reset BIOS Flash Type

	7	6	5	4	3	2	1	0
NetFn/LUN	NetFn = 3Ah (OEM Request)						RsLUN	
Command	Cmd = 01h							
Byte 1	BIOS checksum success/failure indication 00h – Checksum success 01h – Checksum failure							
Byte 1	Completion code							

3.7.2 Get Fibre Channel Port Selection

This command returns the current Fibre Channel port 'routing' selection. The command is available over KCS and IPMB interface.

Table 10. Get Fibre Channel Port Selection

	7	6	5	4	3	2	1	0
NetFn/LUN	NetFn = 3Ah (OEM Request)						RsLUN	
Command	Cmd = 02h							
Byte 1	Intel IANA number (LSB) = 57h							
Byte 2	Intel IANA number = 10h							
Byte 3	Intel IANA number (MSB) = 00h							
Byte 1	Completion code							
Byte 2	Intel IANA number (LSB) = 57h							
Byte 3	Intel IANA number = 10h							
Byte 4	Intel IANA number (MSB) = 00h							
Byte 5	Fiber channel 1 setting, 0=disabled, 1= Front panel, 2= Backplane, 3= reserved.							
Byte 6	Fiber channel 2setting, 0=disabled, 1= Front panel, 2= Backplane, 3= reserved.							

3.7.3 Set Fibre Channel Port Selection

This command sets the Fibre Channel port routing as specified in the request data bytes. The command is available over KCS and IPMB interface.

Table 11. Set Fibre Channel Port Selection

	7	6	5	4	3	2	1	0
NetFn/LUN	NetFn = 3Ah (OEM Request)						RsLUN	
Command	Cmd = 03h							
Byte 1	Intel IANA number (LSB) = 57h							
Byte 2	Intel IANA number = 10h							
Byte 3	Intel IANA number (MSB) = 00h							
Byte 4	Fiber channel 1 setting, 0=disabled, 1=front panel, 2=Backplane, 3= Reserved, FF= Don't change settings,							
Byte 5	Fiber channel 2 setting, 0=disabled, 1=front panel, 2=Backplane, 3= Reserved, FF= Don't change settings,							
Byte 1	Completion code							
Byte 2	Intel IANA number (LSB) = 57h							
Byte 3	Intel IANA number = 10h							
Byte 4	Intel IANA number (MSB) = 00h							

3.7.4 Get HW Fibre Channel Port Selection

This command returns the current Fibre Channel port routing selection as set in the hardware. The command is available over KCS and IPMB interface SetFiberChannelPortSelection.

Table 12. Get HW Fibre Channel Port Selection

	7	6	5	4	3	2	1	0
NetFn/LUN	NetFn = 3Ah (OEM Request)						RsLUN	
Command	Cmd = 04h							
Byte 1	Intel IANA number (LSB) = 57h							
Byte 2	Intel IANA number = 10h							
Byte 3	Intel IANA number (MSB) = 00h							
Byte 1	Completion code							
Byte 2	Intel IANA number (LSB) = 57h							
Byte 3	Intel IANA number = 10h							
Byte 4	Intel IANA number (MSB) = 00h							
Byte 5	Fiber Channel 1 Settings, 1 = Front Panel, 2 = Backplane							
Byte 6	Fiber Channel 2 Settings, 1 = Front Panel, 2 = Backplane							

3.7.5 Set Control State

This command sets the state of a control pin and overrides the control pin's auto state. Refer to Table 15, "Controls Identifier Table" on page 41 for control number information.

Table 13. Set Control State

	7	6	5	4	3	2	1	0
NetFn/LUN	NetFn = 3Eh (OEM Request)						RsLUN	
Command	Cmd = 20h							
Byte 1	Control number							
Byte 2	Control state, 0 = Deassert, 1 = Assert, 3 = Reserved, FF = Don't change settings							
Byte 1	Completion code							

3.7.6 Get Control State

This command sets the state of a control pin. This command overrides the AUTO-state of the control pin. Refer to Table 15, "Controls Identifier Table" on page 41 for control number information.

Table 14. Get Control State

	7	6	5	4	3	2	1	0
NetFn/LUN	NetFn = 3Eh (OEM Request)						RsLUN	
Command	Cmd = 20h							
Byte 1	Control number							
Byte 1	Completion code							
Byte 2	Control state, 0 = Deassert, 1 = Assert, 3 = Reserved, FF = Don't change settings							

3.7.7 Controls Identifier Table

Table 15, "Controls Identifier Table" on page 41 lists the control identifiers that can be used with Set/Get Control State IPMI commands to query or set information on certain controls in the firmware.

Table 15. Controls Identifier Table

Control Description	Control Number
FWH Hub (for BIOS bank information)0	0
FWH 0 Write Protect	1
FWH 1 Write Protect	2
FWH 0 Top Block Lock	3
FWH 1 Top Block Lock4	4

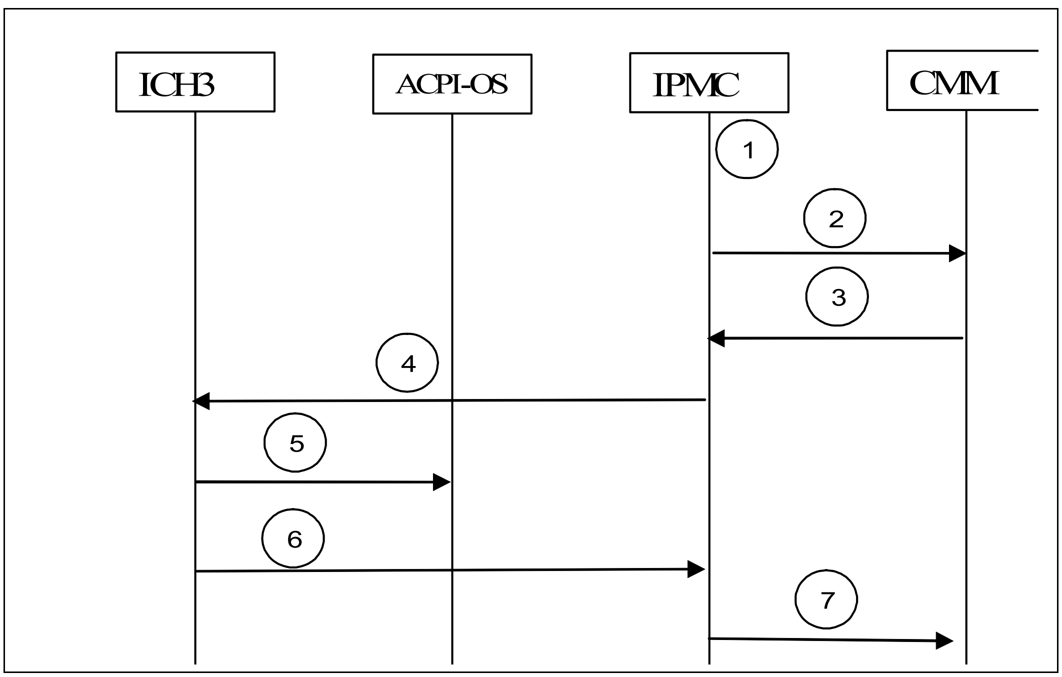
3.7.8 Hot-Swap Process

The AT8000 SBC has the ability to be hot-swapped in and out of a chassis. The onboard IPMC manages the SBC's power-up and power-down transitions. The list below, along with Figure 6, illustrates this process.

1. Ejector latch is opened. HOT_SWAP_PB# assertion. IPMC firmware detects the assertion of this signal.
2. IPMC sends "Deactivation Request" message to CMM. M state moves from M4-> M5.
3. Board moves from M5 -> M6 if the CMM grants the request.
4. The IPMC's ACPI timer (3 minutes) starts if an ACPI-enable OS is loaded. Otherwise, it goes to Step 7 below. The IPMC asserts 20 ms pulse on SMC_PWRBTN#.
5. The Power Button Status register (PWRBTN_STS) is set. It then asserts SCI/SMI# to the OS. If ACPI OS is enabled, SCI interrupt handler on the OS is called. Interrupt handler clears PWRBTN_STS bit. OS starts to perform a graceful shutdown.
6. ICH3 detects "LOW" on the ICH3_PWRBTN#. Asserts ICH3_SLP_S3# and ICH3_SLP_S5# to IPMC. Upon detection of ICH3_SLP_S5# and ICH3_SLP_S3#, board transitions to Step 7 below. If ICH3 doesn't assert the signals, the board will transition to Step 7 below upon the ACPI timer expiration.
7. The firmware deasserts payload power and sets the IPMI locked bit before it transitions from M6 to M1 state.

Note: If the upper-level software moves the IPMC to M6, the same procedure is followed, starting with Step 4.

Figure 6. Hot-Swap Process



3.7.8.1 Hot-Swap LED (DS10)

The AT8000 SBC supports one blue Hot Swap LED, mounted on the front panel. See Figure 12, "AT8000FXX SBC Front Panel" on page 58 for its location. This LED indicates when it is safe to remove the SBC from the chassis. The on-board IPMC drives this LED to indicate the hot-swap state. Refer to Table 16, "Hot-Swap LED (DS11)" on page 43.

When the lower ejector handle is disengaged from the faceplate, the hot swap switch embedded in the PCB will assert a "HOT_SWAP_PB#" signal to the IPMC, and the IPMC will move from the M4 state to the M5 state. At the M5 state, the IPMC will ask the CMM (or Shelf Manager) for permission to move to the M6 state. The Hot Swap LED will indicate this state by blinking on for about 100 milliseconds, followed by 900 milliseconds in the off state. This will occur as long as the SBC remains in the M5 state. Once permission is received from the CMM or higher-level software, the SBC will move to the M6 state.

The CMM or higher level software can reject the request to move to the M6 state. If this occurs, the Hot Swap LED returns to a solid off condition, indicating that the SBC has returned to M4 state.

If the SBC reaches the M6 state, either through an extraction request through the lower ejector handle or a direct command from higher-level software, and an ACPI-enabled OS is loaded on the SBC, the IPMC communicates to the OS that the module must discontinue operation in preparation for removal. The Hot Swap LED continues to flash during this preparation time, just like it does at the M5 state. When main board power is successfully removed from the SBC, the Hot Swap LED remains lit, indicating it is safe to remove the SBC from the chassis.

Warning: Removing the SBC prematurely can lead to device corruption or failure.

Table 16. Hot-Swap LED (DS11)

LED Status	Meaning
Off	Normal status
Blinking Blue	Preparing for removal/insertion: Long blink indicates activation is in progress, short blink when deactivation is in progress.
Solid Blue	Ready for hot swap

3.7.8.2 Ejector Mechanism

In addition to captive retaining screws, the AT8000 SBC has two ejector mechanisms to provide a positive cam action; This ensures the blade is properly seated. The bottom ejector handle also has a switch that is connected to the IPMC to determine if the board has been properly inserted.

3.8 Interrupts and Error Reporting

3.8.1 Device Interrupts

The Low Voltage Intel® Xeon™ processor and E7501 chipset (MCH, ICH3, P64H2) utilize a mechanism for delivering interrupts that is slightly different from, though fully compatible with, previous IA-32 system platforms. The change affects only the delivery mechanism and no changes are required to existing software.

This new delivery mechanism transfers the equivalent APIC messages across the system bus structure rather than using a sideband channel as in the case of the APIC serial bus. There is no longer an APIC bus connection to the processor. This new mechanism improves the interrupt message transfer speed to the processors, thus reducing latency. It also simplifies the flushing of buffers that is required when data is buffered between the I/O subsystem and memory. Since interrupt messages are no longer communicated across a sideband channel, these transfers are now visible to the chipset. The interrupt message transactions themselves can now initiate buffer flushing to ensure all data within the I/O and memory subsystems is coherent.

As before, the LINT[1:0] connections to the processors remain for compatibility with the old PC industry standard, legacy interrupt architecture (8259 controllers). In addition, the P64H2 PCI bridge devices include an interrupt output (BTINTR#), which can be routed into the legacy interrupt controller to facilitate booting from devices residing on the far side of such PCI bridge devices. Once the boot process is complete and the APIC interrupt system is enabled, devices no longer need to share interrupts; This improves interrupt system performance.

The BIOS initializes and enables both the 8259 and APIC but masks all APIC interrupts in the redirection table. This is so the SBC operates in legacy interrupt mode. The BIOS does not operate in APIC mode at any time. An APIC-aware OS disables the 8259 and unmasks the APIC interrupts to switch to APIC mode.

Table 17 displays the interrupt connections provided by the AT8000 SBC. Actual interrupt vector assignments and routing to legacy interrupts as necessary is under BIOS and/or OS control.

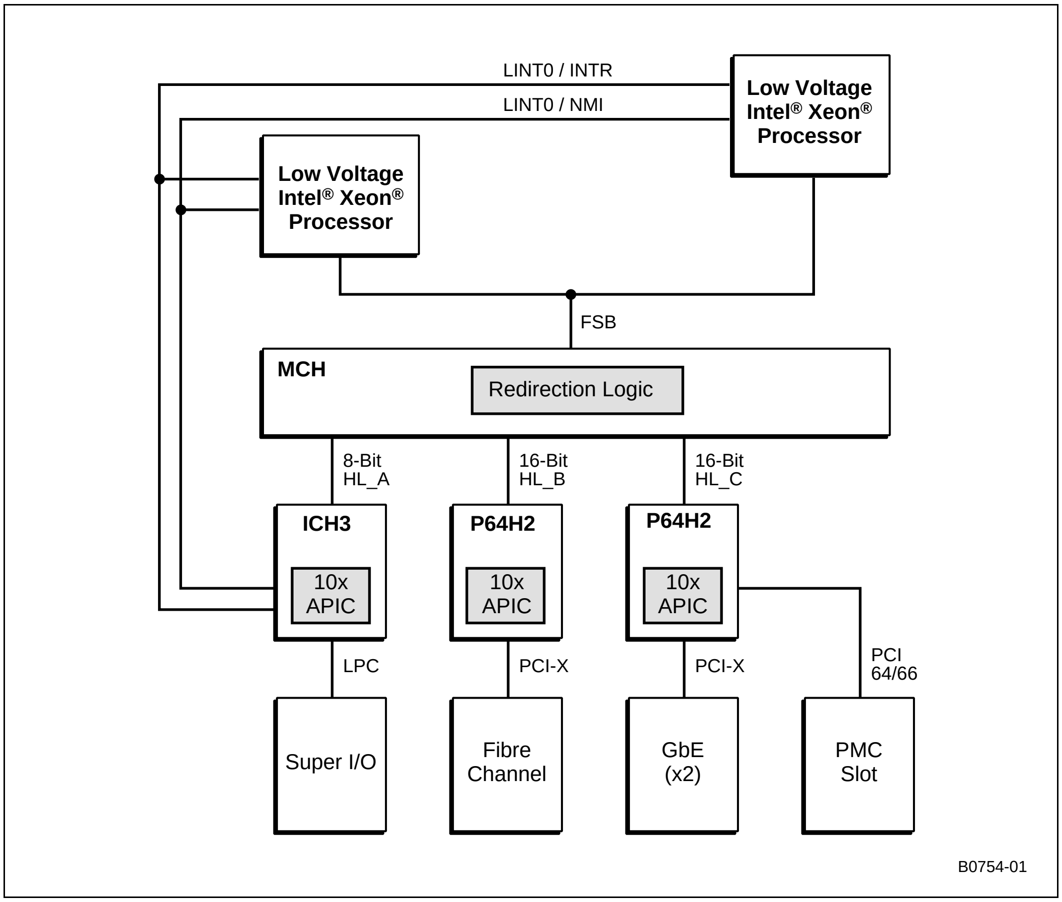
Table 17. Interrupt Assignments (Sheet 1 of 2)

Legacy Interrupt	IRQ assigned
	Master 8259
Internal timer0 output	0
Slave 8259 INTR output	2
Serial Port A	3
	Slave 8259
Internal RTC	0 (8)
Primary IDE	6 (14)
PCI Device Interrupt	IRQ assigned
	HI-A ICH3
Super I/O	SERIRQ
USB 1.1 controller #1	PIRQA#
IPMC_SYSIRQ#	PIRQB#
HI-B P64H2 BTINTR#	PIRQC#
HI-C P64H2 BTINTR#	PIRQD#
	HI-B P64H2
Fibre Channel INTA#	PB_IRQ0
Fibre Channel INTB#	PB_IRQ1
	HI-C P64H2
PMC INTA#	PA_IRQ0
PMC INTB#	PA_IRQ1

Table 17. Interrupt Assignments (Sheet 2 of 2)

Legacy Interrupt	IRQ assigned
PMC INTC#	PA_IRQ2
PMC INTD#	PA_IRQ3
Ethernet #1 INTA#	PB_IRQ0
Ethernet #2 INTA#	PB_IRQ1

Figure 7. Interrupt Signals



3.8.2 Error Reporting

The MCH handles error reporting from the memory subsystem. Errors consist of correctable and uncorrectable bit errors. The ECC algorithms used are capable of correcting any number of bit errors contained within a 4-bit nibble. In addition, any number of bit errors contained within two 4-bit nibbles is detected. The MCH communicates these errors to the ICH3 via special cycles over the hub link interface. These special cycles indicate to the ICH3 that an MCH-detected error has occurred. The MCH special cycle communicates the type of event that should be generated by the ICH3 when an error is detected. Selection for the generation of an SERR, SMI, or SCI event is provided. Status for these reported errors is then found in the MCH DRAM_FERR (first error) and DRAM_NERR (next error) status registers. Refer to the MCH data sheet for more information (see Appendix A, "Reference Documents").

Correctable memory errors generate an SMI and are logged via IPMI as a SEL. Non-correctable errors first generate an SMI (which generates a SEL) and then an NMI.

Each P64H2 device reports the PCI errors that occur on the buses to which it is attached. These consist of the PCI error assertions of the PERR# or SERR# signals. The errors are reported by sending the DO_SERR special cycle to the MCH on the Hub Interface. The MCH forwards the error to the ICH3, which generates the appropriate error condition to the processor(s) such as NMI, SMI, or SCI.

PCI address parity errors are considered catastrophic and may abort further data transfers by the P64H2 if that is the programmed response. Parity/ECC is checked on both the Hub Interface and PCI bus transactions. PCI data parity errors are considered less severe and allow transactions to continue. Data parity errors cause the Detected Parity Error" status to be logged and, if enabled, the DO_SERR special cycle is transmitted. In a transaction where a data error occurs, the data being forwarded to the next bus is "poisoned" to ensure the error follows the data to its destination. Poisoned data has bad parity or multi-bit ECC errors introduced before being forwarded to the next bus.

PCI assertions of the SERR# signal also result in the DO_SERR special cycle being generated on the hub interface when enabled. Other potential causes for a DO_SERR special cycle include:

- Parity errors on the target bus during a write.
- A master timeout on a delayed transaction.
- The occurrence of a PCI master abort cycle.

Refer to the P64H2 Data Sheet, section 4.9, for more information on error handling. For details on obtaining this document, see Appendix A, "Reference Documents."

The ICH3 device has the ability to report PCI and hub link errors directly to the processors. When a PERR# or SERR# occurs on the ICH3 local PCI bus, the ICH3 can be programmed to generate NMI or SMI. The ICH3 also fields messages from the MCH and its attached hub devices to indicate errors to the processors on their behalf. The messages may request SMI#, SCI, NMI, or SERR3 to be asserted. Software must check the MCH and attached hub devices to determine the exact cause of the error. Refer to the ICH3 Data Sheet for more information on error handling and generation. For details on obtaining this document, see Appendix A, "Reference Documents."

3.9 ACPI

ACPI gives the operating system direct control over the power management and Plug and Play functions of a computer. The use of ACPI with theAT8000 SBC requires an operating system that provides ACPI support. ACPI features include:

- Plug and Play (including bus and device enumeration) and APM support (normally contained in the BIOS).
- Power management control of individual devices, add-in boards (some PMC cards may require an ACPI-aware driver), and hard-disk drives.
- A soft-off feature that enables the operating system to power off the computer.
- Support for an IPMC firmware command switch.

3.9.1 System States and Power States

Under ACPI, the operating system directs all system and device power state transitions. The operating system puts devices in and out of low-power states based on user preferences and knowledge of how devices are being used by applications. Devices that are not being used can be turned off. The operating system uses information from applications and user settings to put the system as a whole into a low-power state.

Table 18, "Power States and Targeted System Power" on page 47 lists the power states and the associated system power targets supported by the AT8000 SBC. See the ACPI specification for a complete description of the various system and power states.

3.10 Watchdog Timer

Table 18. Power States and Targeted System Power

Global States	Sleeping States	Processor States	Device States
G0 – working state	S0 – working	C0 – working	D0 – working state.
G1 – sleeping state	S4 – Suspend to disk. Context saved to disk.	No power	D3 – no power except for wake up logic.
G2/S5	S5 – Soft off. Context not saved. Cold boot is required.	No power	D3 – no power except for wake up logic.
G3 – mechanical off AC power is disconnected from the computer.	No power to the system.	No power	D3 – no power for wake up logic, except when provided by battery or external source.

The watchdog timer on the IPMC can be configured and used through standard IPMI v1.5 watchdog timer commands. Refer to Section 3.10.7.1, "WDT #1" on page 52 for detailed implementation.

3.10.1 Reset Logic

The following topics describe the two types of reset requests and the boot relationships among them. The two types of reset requests available on the AT8000 are:

- Hard reset request (always results in a cold boot)
- Soft reset request (can result in either a warm or cold boot)

A hard reset request occurs whenever the processor Reset line is asserted and then deasserted. A soft reset occurs whenever an assertion occurs on the processor Init line. Whenever a soft reset request occurs, the BIOS checks two memory locations to determine whether to initiate a warm boot while leaving main memory intact or a cold boot that clears memory.

Whenever the BIOS detects that the reset is either a hard reset or a cold boot, it specifically clears the memory location 40h:72h so it does not contain a 1234h. Under warm boot conditions, this memory location contains a 1234h (the developer's application writes this value in this location [using /dev/mem] when it is started). If a hard reset occurs (as defined in the hard reset topic below), it is certain that the 40h:72h location contains a non-1234h value.

3.10.2 Hard Reset Request

A Hard Reset, or CPU Reset, is defined as the assertion of the processor reset signal (see Table 19, "Reset Request" on page 49). This initializes the processor state and registers, disables internal caches, and causes the processor to unconditionally begin execution from the reset vector. A hard reset is initiated by the following events:

1. A power up of the SBC. The SMC enables the onboard power supplies.
2. The SMC negates the ICH3_PWROK signal (see Note below).
3. A "reset" command from the Port CF9h I/O register (refer to the "Intel® 82801CA I/O Controller Hub 3 (ICH3-S) Datasheet" for information about this register).
4. Watchdog timer (WDT #1) expires and is configured to initiate a hard reset. See "Watchdog Timers (WDTs)" on page 52 for more information.
5. Watchdog timer (WDT #3) expires after failure to perform the first instruction fetch.

Note: The IPMC can negate the dedicated signal ICH3_PWROK to initiate a processor reset. ICH3_PWROK indicates whether power is OK. If the IPMC deasserts ICH3_PWROK, the hardware asserts the processor reset lines.

3.10.3 Soft Reset Request

The assertion of the processor's INIT signal causes a soft reset or "CPU INIT" (see Table 19, "Reset Request" on page 49). The ICH3 is normally responsible for driving the INIT signal. A CPU INIT event causes the processor(s) to fetch the reset vector at the next instruction boundary. The majority of the processor and all of the cache states are unaffected by an INIT event.

After the INIT event, hardware may be reset (or not reset) under BIOS control. PCI buses are reset using their respective bridge control registers. This signal is then level translated to the processor compatible signal level. INIT may be caused by the following events:

1. The reset button is pressed (see Note below). See "AT8000FXX SBC Front Panel" on page 58 for its location.
2. A processor shutdown special cycle occurred.
3. An INIT command from Port 92h I/O register (refer to the *Intel® 82801CA I/O Controller Hub 3 (ICH3-S) Datasheet* for information about this register).
4. An INIT command from Port CF9h I/O register.
5. A keyboard reset command (ICH3 RCIN# signal asserted).
6. The IPMC may also directly assert the INIT signal; WDT #1 expires and is configured for a soft reset.
7. Processor BIST is enabled and a hard reset is initiated from the Port CF9h register. This asserts the INIT signal but is not classified as a soft reset since CPU reset is also asserted.
8. A processor INIT may also be initiated through an APIC "init" message. This message may target a specific processor or all processors. This "init" is an internally generated event (No INIT signal is asserted) so the IPMC is unable to detect this occurrence.

Note: The reset button (RESET_PB#) is an input to the IPMC. There are also IPMI commands to reset the board and change power states through the software. However, the reset button is a last resort because the user must be physically present at the chassis to reset the board.

After a Soft Reset/CPU Init, the BIOS code executes and determines if the reset is a warm boot or a cold boot. A warm boot restarts the system and keeps memory above the 8 MByte boundary intact. During a warm boot the MCH is not reset, allowing DRAM refresh to continue during and over the soft reset event. A cold boot sets the state of all peripherals to the same state they would be in if a hard reset were triggered.

Table 19. Reset Request

Reset Request	Signal Activated	Type
Hard	Reset	Full reboot
Soft	Init	Partial reboot

3.10.4 Warm Boot

A warm boot occurs when the processor is booting after a soft reset request. To qualify as a warm boot, the reset counter located at 40h:D0h must be non-zero (by default, the reset counter and reset flag are initialized to 10 and 1234h by BIOS after a cold boot.) Execution starts at the reset vector. The BIOS initializes and configures all devices except for memory. Memory contents remain intact except for the first 8 MBytes. The BIOS uses the first 8 MBytes during POST, but does not modify the reset flag or the reset counter. MCH is not reset, allowing DRAM refresh to continue during the warm boot.

Note: On every warm boot, BIOS automatically decrements the reset counter by one. When the reset counter reaches zero and the soft reset is initiated, a cold boot occurs instead of warm boot.

3.10.5 Cold Boot

Any soft reset that does not meet the configuration described in the preceding Warm Boot section is classified as a cold boot. Execution starts at the reset vector, and BIOS initializes and configures all devices, including memory subsystem, as if a hard reset had occurred. See Table 20, “Reset Actions” on page 49.

During a cold boot the BIOS initializes the warm reset counter to 10h and clears the reset flag to 1234h. Software can then read the reset flag to determine the type of reset.

Table 20. Reset Actions

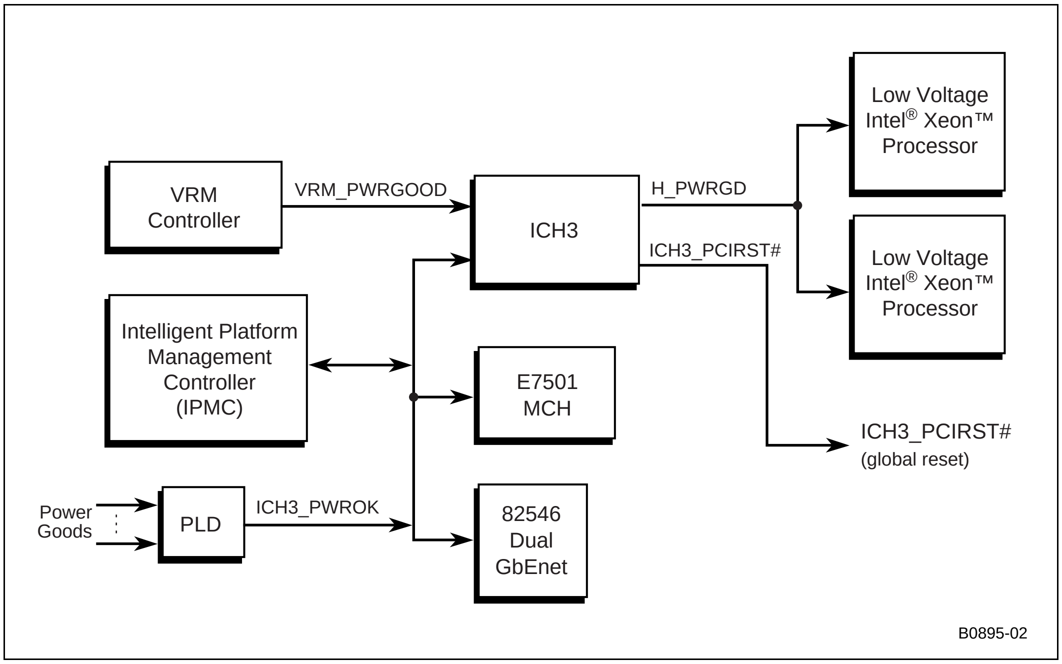
Reset Actions	System Function	Memory Status
Warm boot	Partial restart	Preserves memory above 8MB boundary
Cold boot	Full restart	Functionally equivalent to a hard reset.

3.10.6 Power Good

When the AT8000 SBC is inserted into the chassis, the hardware management circuitry is “hot plugged.” The hardware management voltage is immediately applied, and the on-board IPMC is reset. After the hardware management reset, the operation of the IPMC and full power-up of the SBC are under firmware control.

Upon command to power on the module, the IPMC asserts the "power enable" signal to the on-board DC/DC converters. Full power-up of the SBC is sequenced by hardware to ensure device-specific power requirements are followed. Sequencing of specific voltages is required to ensure that devices using multiple voltages are not damaged or stressed.

Figure 8. Power Good Map



As the many voltages power up, each regulator produces a "power good" signal. All of these power good signals are logically OR'd (with the exception of the VRM power good) to produce the ICH3_PWROK signal input to the ICH3 as shown in Figure 8, Power Good Map. When this signal is active, it indicates all on-board power is good.

Next, the VRM power good is gated with the ICH3_PWROK signal in the ICH3 to produce the processor's power good signal input.

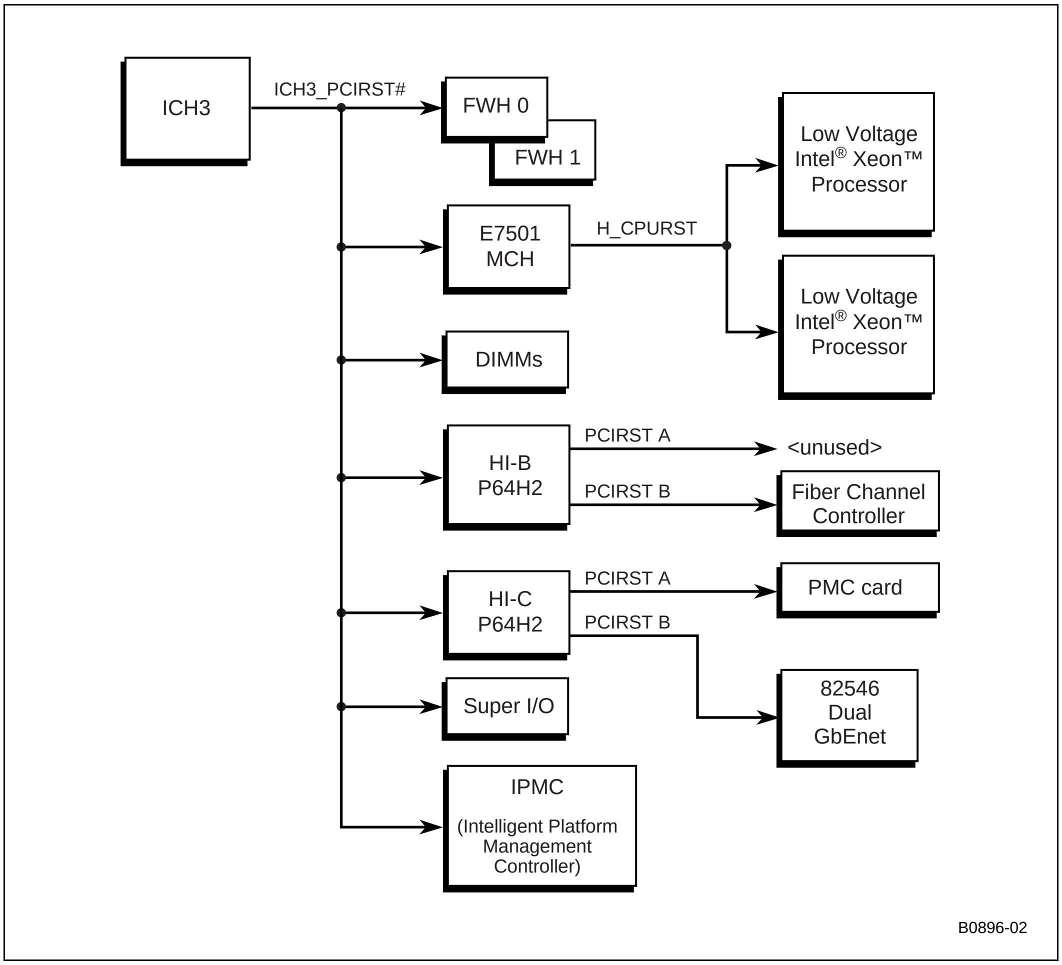
As soon as the ICH3 device is powered, its PCI reset output is asserted. This reset output remains asserted until all power good signals are present (indicated by the ICH3_PWROK signal), the processor VRM power good signal is asserted, and device voltage/clock stabilization times have been satisfied.

Device resets are then released, and processor BIOS execution and boot begins. The PCI reset output of the ICH3 is the source of all other power-up reset signals as shown in Figure 9, "Reset Chain" on page 51

The IPMC is also capable of initiating this power-up or global reset by negating the ICH3_PWROK signal. Additionally, devices on specific PCI buses may be independently reset by software through their associated bridge devices.

When commanded to do so, the IPMC releases device and processor resets, and processor BIOS execution and boot begins.

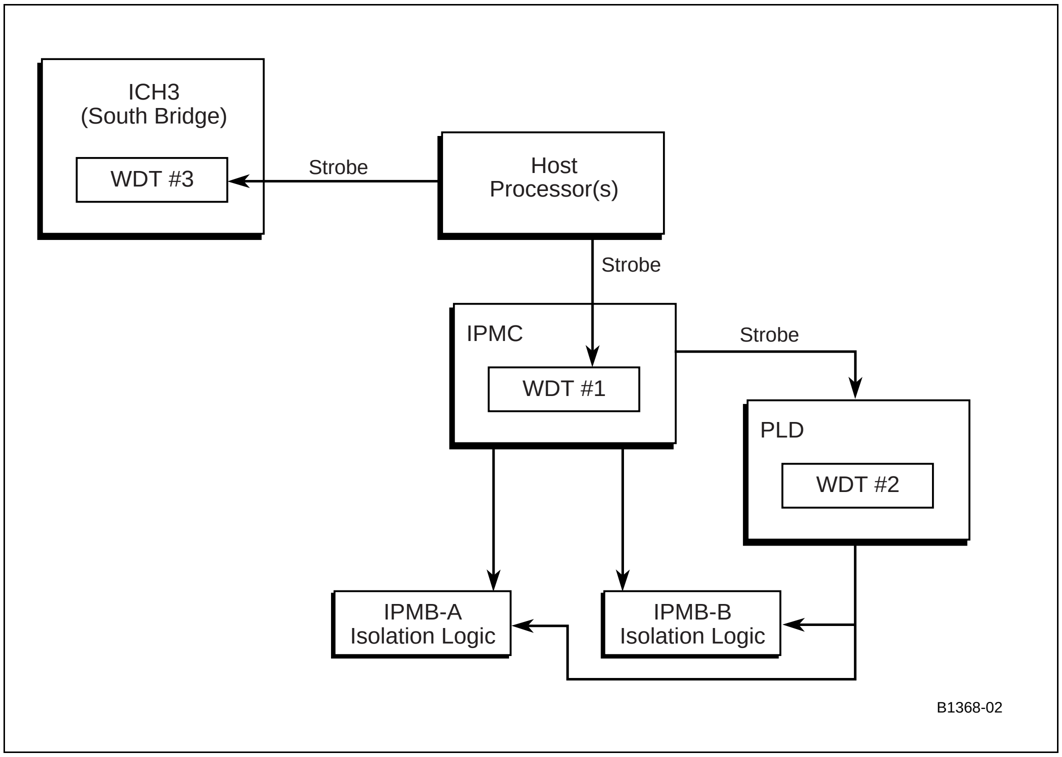
Figure 9. Reset Chain



3.10.7 Watchdog Timers (WDTs)

Figure 10, "Watchdog Timers" on page 52 shows the relationship between the three watchdog timers (WDTs) on the AT8000 SBC.

Figure 10. Watchdog Timers



3.10.7.1 WDT #1

The first WDT (WDT #1) is a hardware timer in the IPMC. WDT #1 is IPMI compliant; its interaction with the host processor BIOS or system software is accomplished through IPMI commands over the Keyboard Controller Style (KCS) interface to the IPMC. The host processor uses the Set Watchdog Timer message to configure WDT #1, then the Reset Watchdog Timer message to strobe the timer.

WDT #1 can be set to any value between 100 ms and 6,553,600 ms in 100 ms intervals. Another configuration parameter is an indicator of which software is controlling WDT #1. This has five state settings:

1. BIOS FRB2: Used during fault-resilient booting to detect issues in the BIOS.
2. BIOS/POST: Used while the BIOS is running through its POST operations.
3. OS Load: Set by the BIOS just before an OS load, then reset by the OS (the OS must be enabled to do so) when it finishes booting.
4. SMS/OS: Used by the system management software or the OS.
5. OEM: Used by any OEM software.

WDT #1 can also be configured to take various actions before timing out (for example, SMI, NMI, nothing) or after timing out (for example, hard reset, power down, or power cycle). In addition, an event can be logged into the SEL whenever the watchdog timer expires. If WDT #1 expires, the IPMC is not reset. For more details on the watchdog timer commands and settings, see the IPMI specification version 1.5.

On power up, the initial state is that the IPMI WDT #1 is not running. Normally some code (BIOS or OS level) must send the Reset Watchdog Timer command to start the timer running. The same code sends a Set Watchdog Timer command first to set up the timer to a known state (see the IPMI specification for more details).

When WDT #1 times out, it logs an event into the SEL, provided that the “Don’t Log” flag is false (see the IPMI 1.5 specification for details). The SEL event also describes the timeout action taken.

If WDT #1 times out and causes a hard reset, the timer state is equivalent to the power-up state (that is, not running; either BIOS or the OS must configure and start it). If the host processor is reset (soft or hard) independent of WDT #1, the firmware disables the watchdog timer.

One of the actions BIOS takes very early in its code is to start the WDT #1 to monitor its boot progress. When it finishes POST, the BIOS turns off WDT #1 during the OS load period.

WDT #1 parameters are altered according to BIOS control parameters, and WDT #1 is not running when the OS first (re)starts. The BIOS sets WDT #1 to a length of time longer than the expected POST time; therefore, BIOS does not actively strobe WDT #1. The flag that determines if a WDT #1 reset must be hard or soft remains over any type of reset, since it is held in the microcontroller.

3.10.7.2 WDT #2

WDT #2 (implemented in a PLD) must be strobed by the IPMC firmware. If WDT #2 expires, it isolates the SBC from the backplane IPMB buses and resets the IPMC. There is no method for the processor to be explicitly notified that the IPMC is reset. Once the IPMC has reset, the main processors can resume communication with the IPMC. The watchdog timer is set to trigger after 96 seconds, and the IPMC strobes it once a second.

WDT #2 is always running; that is, the counter is always counting. However, a PLD component controls the IPMC reset and IPMB isolation associated with WDT #2 expiration, ignoring any WDT event until the IPMC strobes/enables the LTC4300 IPMB interfaces.

3.10.7.3 WDT #3

WDT #3 is contained within the ICH3 device. This watchdog timer monitors the processor’s first attempt to fetch an instruction after a power up or hard reset. If the processor has not fetched its first instruction within the timeout period, the ICH3 resets the processors. Since the processor has not begun any execution, the ICH3 uses a hard reset.

3.10.7.4 Health LED

The AT8000 SBC supports one bicolor health LED to indicate the SBC’s health status, i.e., whether a fault or error condition has been detected on the SBC. This LED is mounted on the front faceplate and driven by the onboard IPMC. The health LED will only be driven to an error condition (red) if there is a critical or non-recoverable (major or critical in ATCA parlance) condition active on the SBC. Alarms could include exceeding sensor thresholds for temperature and on-board logic voltages. The health

LED remains red until the sensors return to a normal operating value. Hard-drive failures, boot failures, etc. are not considered critical/major IPMI states, so the IPMC does not explicitly set the health LED in these cases.

Note: The LED's error state color defaults to red, but the color can be overridden using PICMG 3.0-defined commands.

Table 21. Health LED

LED Status (right)	Meaning
Solid Green	Healthy
Solid Amber/Red	Fault or error condition

The default color and override capabilities of the LED follow the LED management requirements defined in Section 3.2.5 of the PICMG 3.0 specification.

3.10.7.5 OOS (Out Of Service) LED

The AT8000 SBC supports one bicolor "OOS" LED, mounted on the front faceplate. The LED can be driven to display a red or amber color. When this LED is lit, it indicates that the board is not in service. Its back-end (payload) power could be OFF or ON. Often the OOS state is entered when a critical fault occurs on the board. In this state, the back-end (payload) power is turned OFF. A board could be in this state when its back-end power is OFF but healthy, or when a board is fully powered but not yet deployed, or during the reset process.

Note: Do not extract a board unless the Hot Swap LED is lit.

Table 22. OOS LED (DS9)

LED Status (left)	Meaning
Off	In service
Solid Amber/Red	Fault or error condition

The default color and override capabilities of the LED follow the LED management requirements defined in Section 3.2.5 of the PICMG 3.0 specification.

3.10.7.6 Hot-Swap LED

See Section 3.7.8, "Hot-Swap Process" on page 42.

3.10.7.7 IDE Drive Activity LED

Table 23. IDE Drive Activity LED

LED Status	Meaning
Off	Normal/No disk access
Green (Blinking)	Disk access (read/write activity)

3.10.7.8 User Programmable LEDs

The AT8000 SBC provides two bicolor LEDs for user-programmable functions. The LEDs can be driven to display a red, green or amber color. When these LEDs are lit, they indicate a status of a user-defined function.

Table 24. User Programmable LEDs

LED Status (left)	LED Status (right)	Meaning
Off	Off	No Status
Red	Red/Green	Active Status of user defined function

The user-programmable LEDs are connected to the GPIO pins on the ICH3 device as follows:

Table 25. GPIO Pin Connections

LED	Pin
User_Prog_LED1_Red#	GPIO21
User_Prog_LED1_GRN#	GPIO20
User_Prog_LED2_Red#	GPIO28
User_Prog_LED2_GRN#	GPIO23

By programming the ICH3 GPIO registers as outputs, then selecting the appropriate state (low for illumination, high for off), the user enables the LEDs as required. Refer to the ICH3 datasheet in appendix B for specific GPIO 20, 21, 23, 28 register information.

3.10.7.9 Network Link/Speed LEDs

The front panel of the SBC provides two LEDs for each Ethernet connection indicating the speed and link activity for that network connection:

Table 26. Network Link LEDs

Link LED Status (left)	Meaning
Off	No link
Solid Green	Link established
Blinking Green	Link with activity

Table 27. Network Speed LEDs

Speed LED Status (right)	Meaning
Off	10 Mbps connection
Solid Green	100 Mbps connection
Solid Yellow	1000 Mbps connection

3.10.7.10 Network Controller Port State LEDs

The front panel of the SBC provides a bicolor LED for each Ethernet channel that can light to indicate the Ethernet port state. These LEDs can display a red, green or amber color. The function of the port state LEDs is user definable. The Ethernet Controller SDP[6:7] GPIO bits for each channel are the outputs that control the LEDs. SDP[6] is connected to the Green LED, and SPD[7] is connected to the Red LED.

Refer to the documentation for the Intel® 82546 Dual Gigabit Ethernet Controller for information on how to drive these LED signals. Note that existing network drivers may drive these GPIO pins.

Table 28. Ethernet Controller Port State LED

LED Status (right)	Meaning
Off	No Status
Red/Green/Amber	Active status of user-defined function

3.10.7.11 Fibre Channel Port State LEDs

The AT8000 SBC supports two Fibre Channel port state LEDs mounted on the front faceplate. The LEDs are green and yellow. When this LED is lit, it indicates the port state of each Fibre Channel port. LED states are shown in the table as follows:

Table 29. Fibre Channel Port State LED (DS2, DS3)

Yellow LED Status (Fibre Channel 1, left)	Green LED Status (Fibre Channel 2, right)	Meaning
ON	ON	Power On
Flashing	OFF	Loss-of-Sync
ON	OFF	Signal Acquired
OFF	ON	On-Line
FLASH	FLASH	F/W Error

Connectors 4

Connectors along the rear edge of ATCA* server blades are divided into three distinct zones, as described in Section 2.3 of the *PICMG* 3.0 Specification*.

- Zone 1 for system management and power distribution
- Zone 2 for data fabric
- Zone 3 for the rear transition module.

As shown in Figure 11, the AT8000 includes several connectors to interface with application-specific devices. Some of the connectors are available at the front panel.Each connector is described briefly in Table 31 on page 60. A detailed description and pinout for each connector is found in the following sections

Figure 11. AT8000 SBC Connector Locations

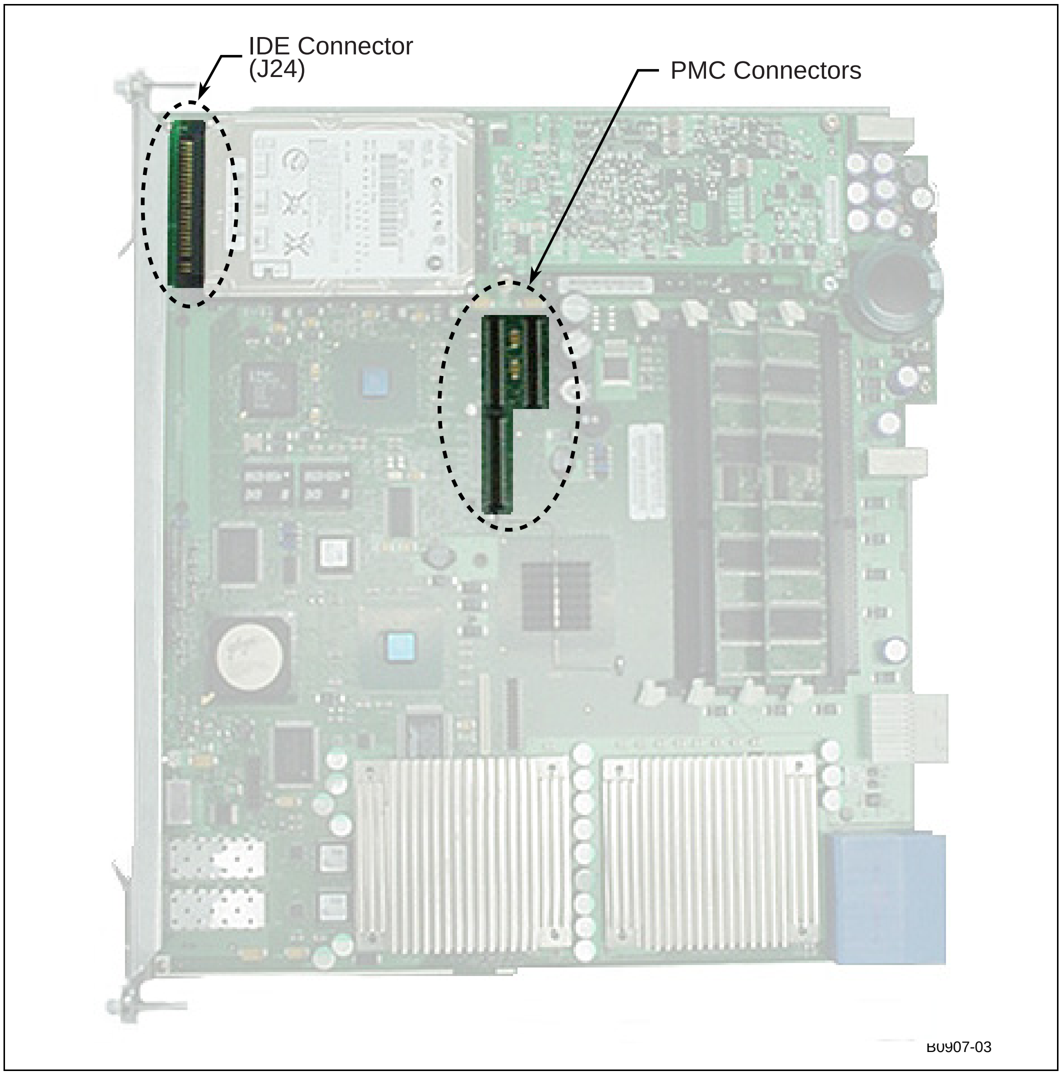


Figure 12. AT8000FXX SBC Front Panel

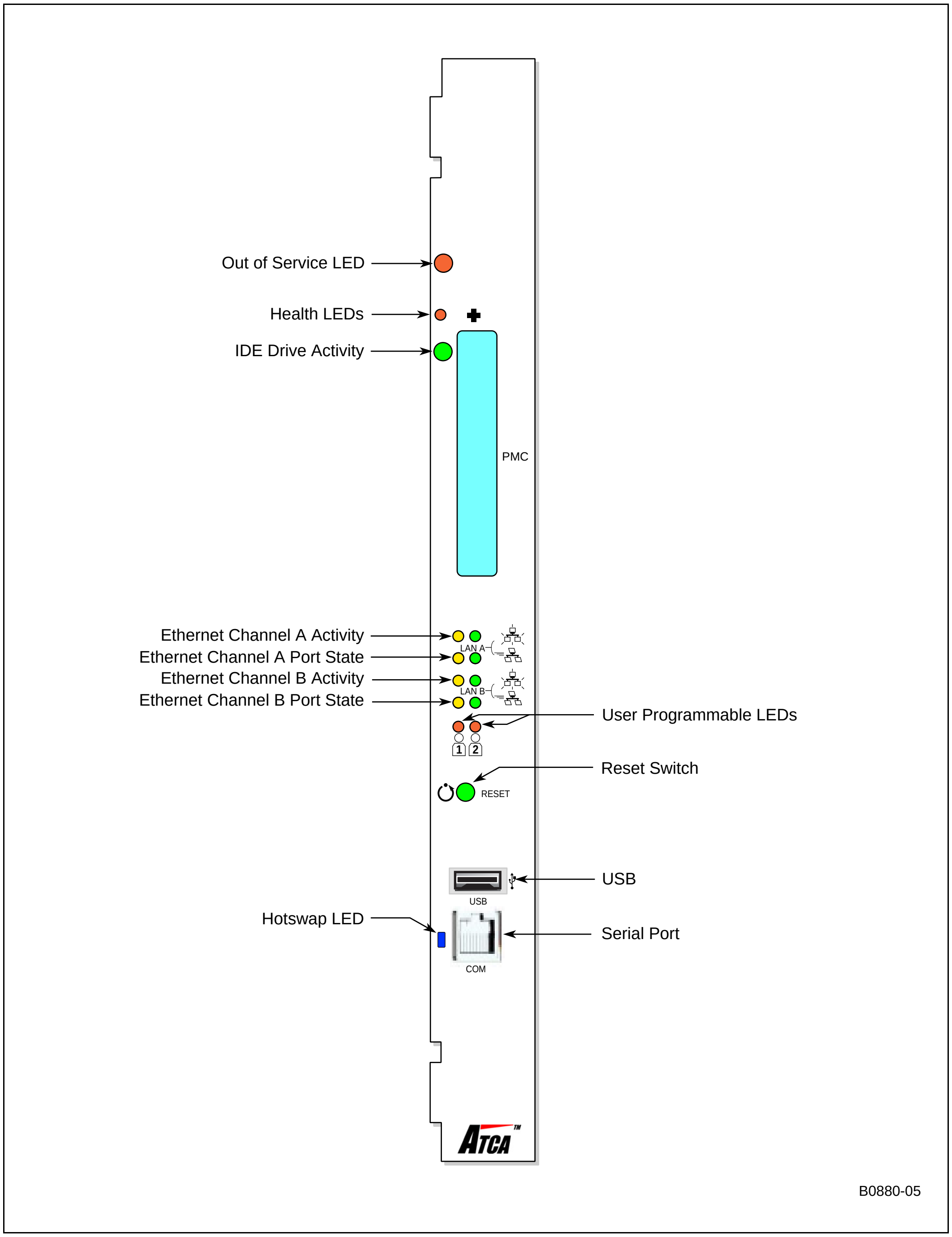


Figure 13. AT8000NXX SBC Front Panel

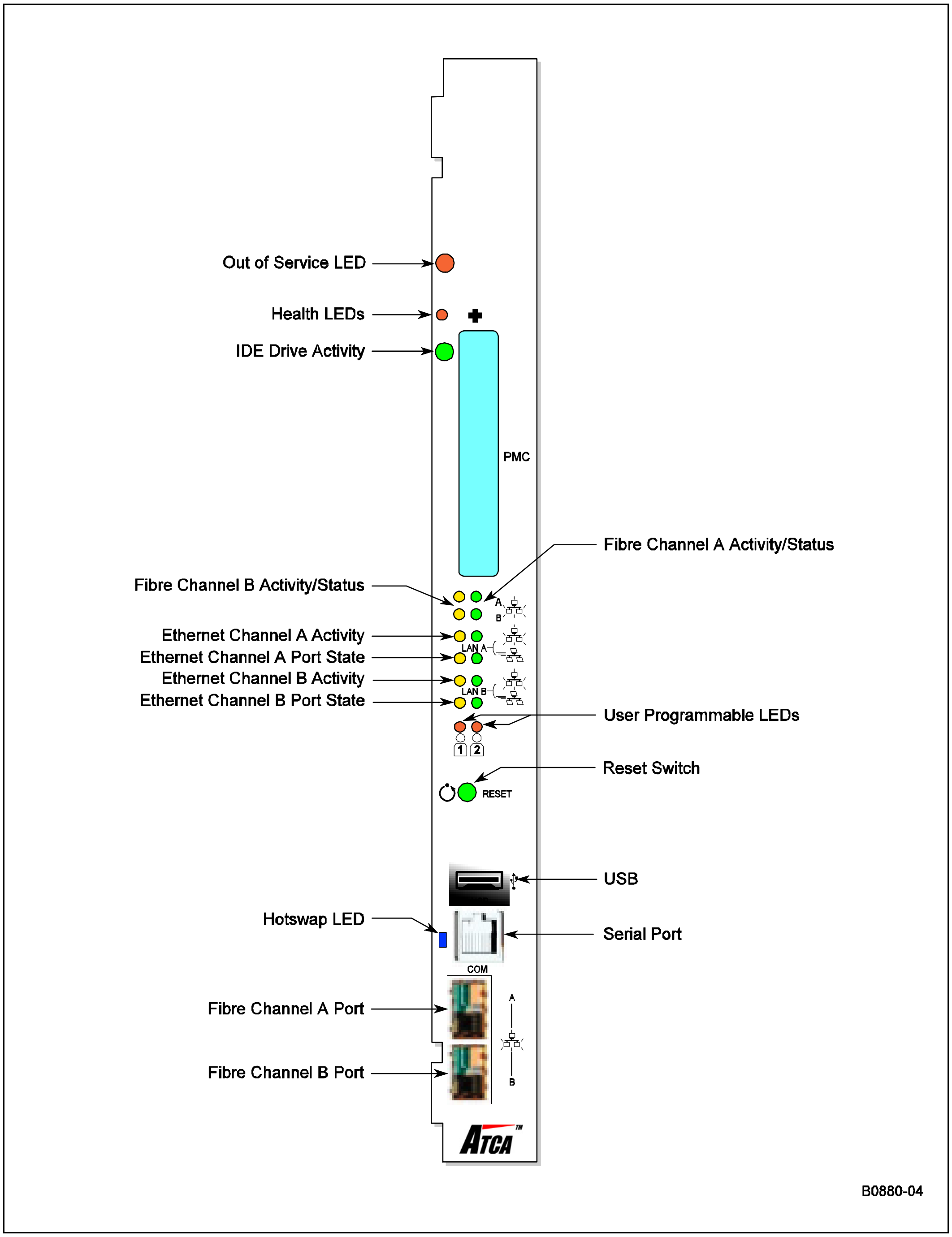


Table 30. LED Descriptions

LED	Description
OOS	Out of Service, bicolor
	Health, bicolor
IDE Drive Activity	Lights when drive activity occurs.
FC1	Fibre Channel 1 Activity and Status bicolor Yellow /Green
FC2	Fibre Channel 2 Activity and Status bicolor Yellow / Green
 A	Gigabit channel 1, Gigabit Linkup (Activity) Port State / Link
	Gigabit channel 1 Link 1000 (yellow)/Link 100 (Green) Yellow /Green
 B	Gigabit channel 2, Gigabit Linkup (Activity) Port State / Link
	Gigabit channel 2 Link 1000 (yellow) /Link 100 (Green) Yellow / Green
	User Programmable bicolor LEDs
	Hot Swap LED

Table 31. Connector Assignments

Backplane Connectors	Description	Details
P1	Mezzanine connector P1	2X30 SMT, 60 pin
P2	Mezzanine connector P2	2X30 SMT, 60 pin
P10	Positronic Power Connector	34 pin
P23	Data Transport Connector (Zone 2)	Two 10/100/1000 Ethernet ports Two 2 Gbit Fibre Channel ports
Front Panel Connectors	**Description**	**Details**
J12	USB Connector	USB Connector
J17	Serial Port Connector	Serial Port Connector
J25, 26, 27	PMC Connectors	PMC Connectors
J34, J35	Fibre Channel 1 (SFP1), Fibre Channel 2 (SFP2)	SFP Receptacle

4.1 Backplane Connectors

4.1.1 Power Distribution Connector (Zone 1)

Zone 1 consists of P10, a 34-pin Positronic header connector that provides the following signals:

- Two -48 VDC power feeds (four signals each; eight signals total)
- Two IPMB ports (two signals each, four signals total)
- Geographic address (eight signals)
- 5.55 Amperes are allocated to AT8000 on the -48 VDC redundant power feeds. This is equivalent to 200 Watts at the minimum input voltage (-36 VDC). The Zone 1 connector and pin out is compatible with the backplane for *Intel® Netstructure™ MPCHC0001 14U Shelf Technical Product Specification*.

Note: The analog test and ring voltage pins defined on P10 are left unconnected on AT8000.

The connector used is Positronic part number VPB30W8M6200A1. Figure 14, “Power Distribution Connector (Zone 1) P10” on page 61 shows the mechanical drawing of the connector. The pin assignments are given in Figure 32, “Power Distribution Connector (Zone 1) P10 Pin Assignments” on page 61.

Figure 14. Power Distribution Connector (Zone 1) P10

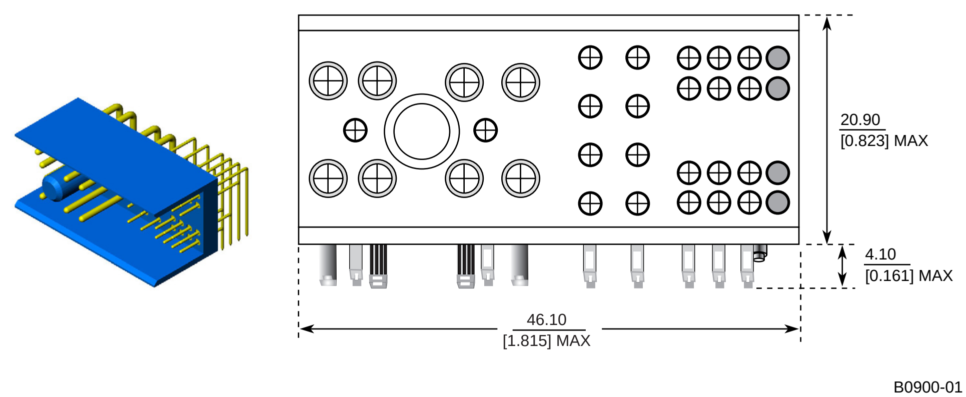


Table 32. Power Distribution Connector (Zone 1) P10 Pin Assignments

Pin #	Signal Name	Description	Pin #	Signal Name	Description
1	Reserved	No Connect	18	Unused	No Connect
2	Reserved	No Connect	19	Unused	No Connect
3	Reserved	No Connect	20	Unused	No Connect
4	Reserved	No Connect	21	Unused	No Connect
5	GA0	Geographic Addr Bit 0	22	Unused	No Connect
6	GA1	Geographic Addr Bit 1	23	Unused	No Connect
7	GA2	Geographic Addr Bit 2	24	Unused	No Connect

Table 32. Power Distribution Connector (Zone 1) P10 Pin Assignments

8	GA3	Geographic Addr Bit 3	25	EMI_GND	EMI Chassis Ground
9	GA4	Geographic Addr Bit 4	26	LOGIC_GND	Gnd Ref for Card Logic
10	GA5	Geographic Addr Bit 5	27	ENABLE_B	Enb DC-DC conv, B Feed
11	GA6	Geographic Addr Bit 6	28	VRTN_A	-48 V Return, Feed A
12	GA7/P	Geo Adr Bit 7 (Odd Parity)	29	VRTN_B	-48 V Return, Feed B
13	IPMB_CLK_A	IPMB Bus A Clock	30	- 48 V_EARLY_A	-48 V In, Feed A Precharge
14	IPMB_DAT_A	IPMB Bus A Data	31	-48 V_EARLY_B	-48 V In, Feed B Precharge
15	IPMB_CLK_B	IPMB Bus B Clock	32	ENABLE_A	Enb DC-DC conv, A Feed
16	IPMB_DAT_B	IPMB Bus B Data	33	-48V_A	-48 V Input, Feed A
17	Unused	No Connect	34	-48V_B	-48 V Input, Feed B

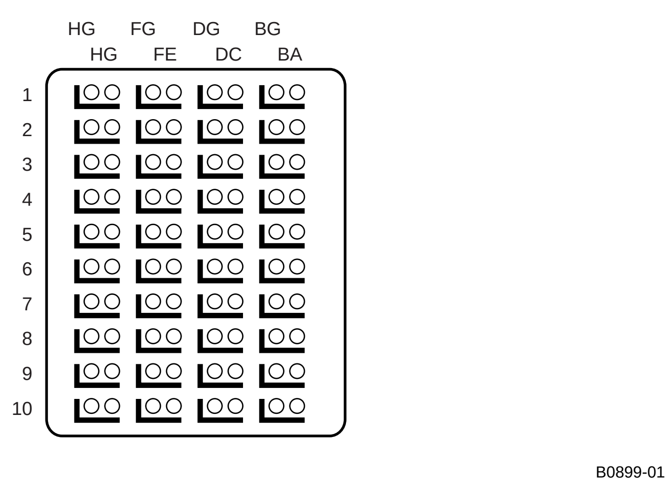
4.1.2 Data Transport Connector (Zone 2)

Zone 2 consists of one 120-pin HM-Zd connector, labeled P23, with 40 differential pairs. This data transport connector provides the following signals:

- Two 10/100/1000Base-T/TX Ethernet base fabric channels (four differential signal pairs each, 16 signals total).
- Two 2 Gbit Fibre Channel ports on the extended fabric (two differential signal pairs each, eight signals total).

The connector used is AMP/Tyco part number 1469001-1, Intel part number A66621-001. Figure 15, "Data Transport Connector (Zone 2) J23" on page 62 shows a face view of the connector.

Figure 15. Data Transport Connector (Zone 2) J23



The following naming convention describes the signals on this connector. Signal direction is defined from the perspective of AT8000.

P[C]dxp where:

P = Prefix (B=Base Interface [Gigabit Ethernet], F= Fabric Interface [Fibre Channel])

C = Channel (1-2)

d = direction (Tx = Transmit, Rx = Receive)

x = port number (0-1)

Note: A port is two differential pairs, one Tx and one Rx

p = polarity (+, -)

The BG, DG, FG and HG (G for Ground) columns contain the ground shields for the four columns of differential pairs. They have been omitted from the pin out tables below for simplification. All pins in the BG, DG, FG and HG columns are connected to Logic Ground. The used base fabric (Gigabit Ethernet) channels are shown in light gray while the used extended fabric (Fibre Channel) ports appear in dark gray.

Table 33. Data Transport Connector (Zone 2) P23 Pin Assignments

Pin	A	B	C	D	E	F	G	H
1	No Connect	No Connect	No Connect	No Connect	F[2]Tx0+	F[2]Tx0-	F[2]Rx0+	F[2]Rx0-
2	No Connect	No Connect	No Connect	No Connect	No Connect	No Connect	No Connect	No Connect
3	No Connect	No Connect	No Connect	No Connect	F[1]Tx0+	F[1]Tx0-	F[1]Rx0+	F[1]Rx0-
4	No Connect	No Connect	No Connect	No Connect	No Connect	No Connect	No Connect	No Connect
5	B[1]Tx0+	B[1]Tx0-	B[1]Rx0+	B[1]Rx0-	B[1]Tx1+	B[1]Tx1-	B[1]Rx1+	B[1]Rx1-
6	B[2]Tx0+	B[2]Tx0-	B[2]Rx0+	B[2]Rx0-	B[2]Tx1+	B[2]Tx1-	B[2]Rx1+	B[2]Rx1-
7	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved
8	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved
9	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved
10	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved

4.1.3 Alignment Blocks

The AT8000 SBC implements the K1 and K2 alignment blocks at the top of Zone 2 and Zone 3, as required in section 2.4.4 of the PICMG 3.0 specification. These are identified on the silkscreen as GP1 and GP2. GP1 provides the PICMG 3.0-mandated keying value of 11, and is either a Tyco* 1469373 or a Tyco 1469268 component (or equivalent). GP2 has a solid face and is used to ensure that RTMs with protruding connectors are not plugged into the AT8000 SBC or vice versa; the component used for this is either a Tyco 1469374 or a Tyco 1469275-2 (or equivalent).

4.2 Front Panel Connectors

4.2.1 USB Connector (J12)

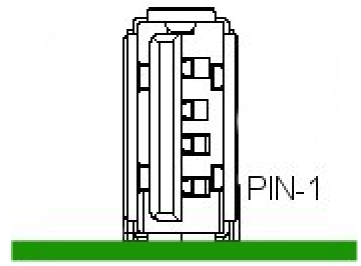
MOLEX part Number: 67329-0020

The AT8000 SBC has one vertical USB connector that supports USB 1.1. USB connector JX is available at the front panel, as shown in Figure 11, "AT8000 SBC Connector Locations" on page 57. The figure shows its position on the board. See Table 34, "USB Connector (J12) Pin Assignments" on page 64 for pinout information.

Table 34. USB Connector (J12) Pin Assignments

USB CONNECTOR	
Pin #	**Signal Name**
1	+5 V
2	-DATA
3	+DATA
4	GND

USB Connector (J12)



4.2.2 Serial Port Connector (J17)

A single serial port interface is provided on the front edge of the card using an RJ-45 style shielded connector. See Figure 11, "AT8000 SBC Connector Locations" on page 57 for its position on the board. The default connector is an 8-pin RJ-45.

MOLEX Part Number 43249-8919

Figure 16. Serial Port Connector (J17)

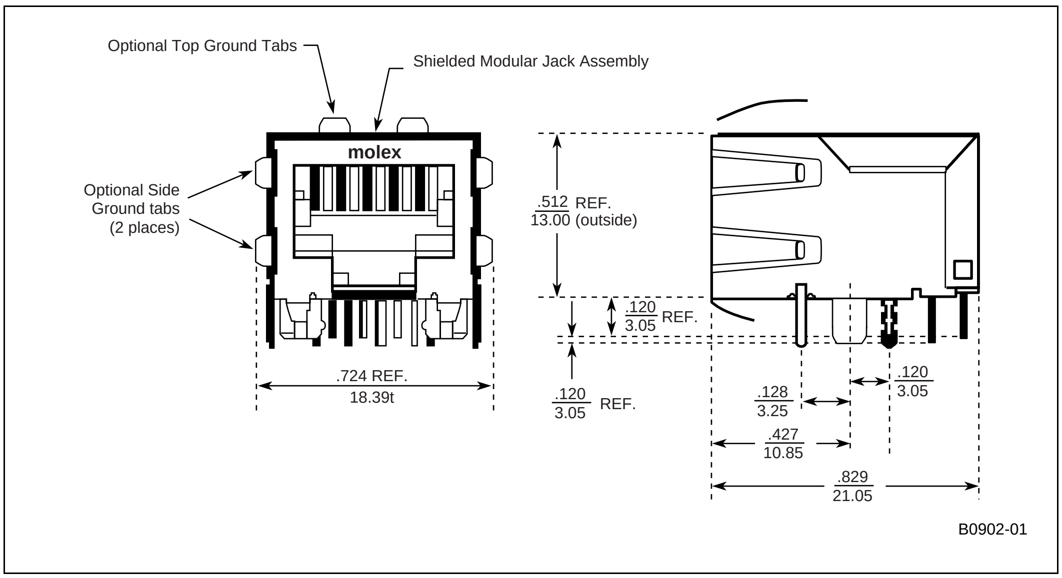
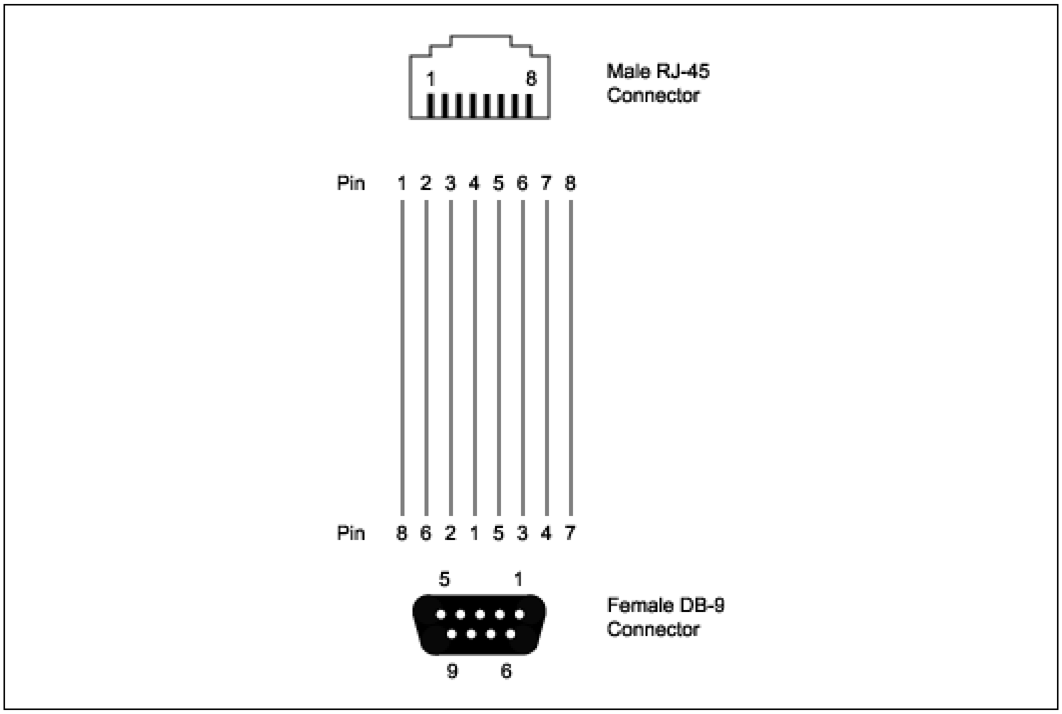


Table 35. Serial Port Connector (J17) Pin Assignments

Connector Pin Number	Serial Port Signal
1	RTS
2	DTR
3	TXD
4	GND
5	GND
6	RXD
7	DSR
8	CTS

Figure 17. DB9 to RJ-45 Pin Translation



4.2.3 Fibre Channel Small Form-Factor Pluggable (SFP) Receptacle (J34 and J35)

AMP part number: 1367073-1

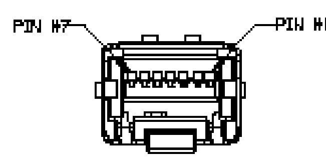
The AT8000 SBC has two SFP receptacles that support either the copper or fiber module interface. Fibre Channel connector J34 and J35 are available at the front panel. See Figure 11, "AT8000 SBC Connector Locations" on page 57 for its position on the board. See Table 37, "Fibre Channel SFP Pin Assignments" on page 67 for pinout information.

Table 36. Fibre Channel SFP Copper Transceiver Module (AMP, J34, J35)

USFibre Channel Connector (J34) Pin Assignments

Fibre Channel CONNECTOR	
Pin #	Signal Name
1	Signal Ground
2	Transmitter Fault
3	Transmitter Disable Input
4	Module Definition 2
5	Module Definition 1
6	Module Definition 0
7	Rate Select (not implemented)
8	Loss of Signal
9	Signal Ground
10	Signal Ground
11	Signal Ground
12	Received Data Out Bar
13	Received Data Out
14	Signal Ground
15	Receiver Power Supply
16	Transmitter Power Supply
17	Signal Ground
18	Transmitter Data In
19	Transmitter Data In Bar
20	Signal Ground

Fibre Channel SFP Receptacle (J34, J35)



4.2.4 Fibre Channel SFP Optical Transceiver Module

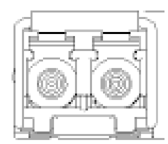
Refer to the Intel® NetStructure™ AT8000 Compatibility Report for a list of SFP optical transceivers that have been validated. The report can be downloaded from http://www.intel.com/design/network/products/cbp/atca/MPCBL0001.htm

Table 37. Fibre Channel SFP Pin Assignments

USFibre Channel Connector (J34, J35) Pin Assignments

Fibre Channel CONNECTOR	
Pin #	Signal Name
1	Transmitter Ground
2	Transmitter Fault (not supported)
3	Transmitter disable
4	Module Definition 2
5	Module Definition 1
6	Module Definition 0
7	Rate Select
8	Loss of Signal Indication
9	Receiver Ground
10	Receiver Ground
11	Receiver Ground
12	Receiver Inverted DATA Out
13	Receiver Non-Inverted DATA Out
14	Receiver Ground
15	Receiver Power Supply
16	Transmitter Power Supply
17	Transmitter Ground
18	Transmitter Non-Inverted DATA In
19	Transmitter Inverted DATA In
20	Transmitter Ground

Fibre Channel SFP Optical Transceiver Module (J34, J35)



4.2.5 PMC Connectors (J25, J26, J27)

There are three 64-pin connectors that make up the PMC card connection:

MOLEX Part Number: 71439-0864

These connectors and pinouts are defined by the following industry standard specifications:

- Draft Standard Physical and Environmental Layers for PCI Mezzanine Cards: PMC IEEE (MMSC) P1386.1/Draft 2.3, October 9, 2000
- Draft Standard for a Common Mezzanine Card Family: CMC IEEE (MMSC) P1386/Draft 2.3, October 9, 2000

The PMC slot is available at the front panel. See Figure 11, “AT8000 SBC Connector Locations” on page 57 for their positions on the board. Pin assignments are listed in Table 38, “PMC Connector Pin Assignments - 32 Bit” on page 68 and Table 39, “PMC Connector Pin Assignments - 64 Bit” on page 69.

Table 38. PMC Connector Pin Assignments - 32 Bit

J25		32 Bit PCI		J26		32 Bit PCI	
Pin	**Signal**	**Signal**	**Pin**	**Pin**	**Signal**	**Signal**	**Pin**
1	TCK	-12 V	2	1	+12 V	TRST#	2
3	Ground	INTA#	4	3	TMS	TDO	4
5	INTB#	INTC#	6	5	TDI	Ground	6
7	BUSMODE1#	+5 V	8	7	Ground	PCI-RSVD	8
9	INTD#	PCI-RSVD	10	9	PCI-RSVD	PCI-RSVD	10
11	Ground	(n/c) 3.3 Vaux	12	11	BUSMODE2#	+3.3 V	12
13	CLK	Ground	14	13	RST#	BUSMODE3#	14
15	Ground	GNT[0]#	16	15	+3.3 V	BUSMODE4#	16
17	REQ[0]#	+5 V	18	17	PME#	Ground	18
19	+3.3V (V I/O)	AD[31]	20	19	AD[30]	AD[29]	20
21	AD[28]	AD[27]	22	21	Ground	AD[26]	22
23	AD[25]	Ground	24	23	AD[24]	+3.3 V	24
25	Ground	C/BE[3]#	26	25	IDSEL (AD17)	AD[23]	26
27	AD[22]	AD[21]	28	27	+3.3 V	AD[20]	28
29	AD[19]	+5 V	30	29	AD[18]	Ground	30
31	+3.3V (V I/O)	AD[17]	32	31	AD[16]	C/BE[2]#	32
33	FRAME#	Ground	34	33	Ground	PMC-RSVD	34
35	Ground	IRDY#	36	35	TRDY#	+3.3 V	36
37	DEVSEL#	+5 V	38	37	Ground	STOP#	38
39	Ground	LOCK#	40	39	PERR#	Ground	40
41	PCI-RSVD	PCI-RSVD	42	41	+3.3V	SERR#	42
43	PAR	Ground	44	43	C/BE[1]#	Ground	44
45	+3.3 V (V I/O)	AD[15]	46	45	AD[14]	AD[13]	46
47	AD[12]	AD[11]	48	47	M66EN	AD[10]	48
49	AD[09]	+5 V	50	49	AD[08]	+3.3 V	50
51	Ground	C/BE[0]#	52	51	AD[07]	PMC-RSVD	52
53	AD[06]	AD[05]	54	53	+3.3V	PMC-RSVD	54
55	AD[04]	Ground	56	55	PMC-RSVD	Ground	56
57	+3.3 V (V I/O)	AD[03]	58	57	PMC-RSVD	PMC-RSVD	58
59	AD[02]	AD[01]	60	59	Ground	PMC-RSVD	60
61	AD[00]	+5 V	62	61	ACK64#	+3.3 V	62
63	Ground	REQ64#	64	63	Ground	PMC-RSVD	64

Table 39. PMC Connector Pin Assignments - 64 Bit

J27		64 Bit PCI	
Pin	Signal	Signal	Pin
1	PCI-RSVD	Ground	2
3	Ground	C/BE[7]#	4
5	C/BE[6]#	C/BE[5]#	6
7	C/BE[4]#	Ground	8
9	+3.3 V (V I/O)	PAR64	10
11	AD[63]	AD[62]	12
13	AD[61]	Ground	14
15	Ground	AD[60]	16
17	AD[59]	AD[58]	18
19	AD[57]	Ground	20
21	+3.3 V (V I/O)	AD[56]	22
23	AD[55]	AD[54]	24
25	AD[53]	Ground	26
27	Ground	AD[52]	28
29	AD[51]	AD[50]	30
31	AD[49]	Ground	32
33	Ground	AD[48]	34
35	AD[47]	AD[46]	36
37	AD[45]	Ground	38
39	+3.3 V (V I/O)	AD[44]	40
41	AD[43]	AD[42]	42
43	AD[41]	Ground	44
45	Ground	AD[40]	46
47	AD[39]	AD[38]	48
49	AD[37]	Ground	50
51	Ground	AD[36]	52
53	AD[35]	AD[34]	54
55	AD[33]	Ground	56
57	+3.3 V (V I/O)	AD[32]	58
59	PCI-RSVD	PCI-RSVD	60
61	PCI-RSVD	Ground	62
63	Ground	PCI-RSVD	64

Addressing 5

5.1 PCI Configuration Map

Table 40, “PCI Configuration Map” on page 71 lists all PCI devices and the bus on which they reside. Note the bus numbers that appear in the table are offset if additional PCI bridge devices are installed in the PMC slot. The bus numbers in parentheses indicate the bus number when no additional PCI bridges are present.

Table 40. PCI Configuration Map (Sheet 1 of 2)

Device	PCI Bus #	PCI Device #	PCI Function #	PCI Device ID	Function Description
MCH	0	0	0	8086/254C	MCH DRAM controller, 8-bit HI-A
MCH	0	0	1	8086/2541	MEM/HI-A Error notification/ configuration
MCH	0	2	0	8086/2543	HI-B, 16-bit Hub Link - PCI bridge
MCH	0	2	1	8086/2544	HI-B error configuration
MCH	0	2	7		HI-B error configuration (SMB shadow)
MCH	0	3	0	8086/2545	HI-C, 16-bit Hub Link - PCI bridge
MCH	0	3	1	8086/2546	HI-C error configuration
MCH	0	3	7		HI-C error configuration (SMB shadow)
MCH	0	4	0	8086/2547	HI-D, 16-bit Hub Link - PCI bridge (Not Used)
MCH	0	4	1	8086/2548	HI-D error configuration (Not Used)
MCH	0	4	7		HI-D error configuration (SMB shadow) (Not Used)
ICH3	0	29	0	8086/2482	USB 1.1 UHCI controller 1, port 0/1
ICH3	0	29	1	8086/2484	USB 1.1 UHCI controller 2, port 2/3 (not used)
ICH3	0	29	2	8086/2487	USB 1.1 UHCI controller 3, port 4/5 (not used)
ICH3	0	30	0	8086/244E	HI-to-PCI bridge
ICH3	0	31	0	8086/2480	PCI-to-LPC bridge and system management, legacy devices
ICH3	0	31	1	8086/248B	IDE controller
ICH3	0	31	3	8086/2483	SMBus 2.0 controller
ICH3	0	31	5	8086/2485	AC’97 Audio (not used)
ICH3	0	31	6	8086/2486	AC’97 Modem (not used)
ICH3	1	8	0	=PHY	Integrated LAN controller (not used)

Table 40. PCI Configuration Map (Sheet 2 of 2)

Device	PCI Bus #	PCI Device #	PCI Function #	PCI Device ID	Function Description
P64H2	C/B (2/5)	31	0	8086/1460	HI-to-PCI bus A bridge
P64H2	C/B (2/5)	29	0	8086/1460	HI-to-PCI bus B bridge
P64H2	C/B+1 (3/6)	31	0	8086/1462	Hot Plug controller (not used)
P64H2	C/B (2/5)	28	0	8086/1461	PCI-B I/OxAPIC Interrupt Controller
P64H2	C/B (2/5)	30	0	8086/1461	PCI-A I/OxAPIC Interrupt Controller
Fibre Channel	B+2 (7)	1 (IDSEL 17)	0/1	1077/2312	Fibre Channel Ports 0/1
Gbit Ethernet	C+2 (4)	1 (IDSEL 17)	0	8086/1010	82546 Gigabit Ethernet Controller #1
Gbit Ethernet	C+2 (4)	1 (IDSEL 17)	0	8086/1010	82546 Gigabit Ethernet Controller #2
PMC	C+1 (3)	1 (IDSEL 17)	-	-	PMC plug-in card; function(s) defined by PMC card

5.2 Configuration Registers

5.2.1 Configuration Address Register MCH CONFIG_ADDRESS

I/O Address: 0x0CF8 Accessed as a Dword

Default Value: 0x00000000

Access: Read/Write

Size: 32 bits

CONFIG_ADDRESS is a 32-bit I/O register that can be accessed only as a Dword. A byte or word reference passes through the Configuration Address Register and hub link interface HI_A onto the PCI_A bus as an I/O cycle. The CONFIG_ADDRESS register contains the Bus Number, Device Number, Function Number, and Register Number for which a subsequent PCI configuration access is intended. This register is defined by the PCI Bus specification.

Table 41. Configuration Address Register Bit Assignments

Bit	31	30 24	23 16	15 11	10 8	7 2	1 0	
	0	R	0	0	0	0	R	Default

Bit	Description
31	Configuration Enable (CFGE): When this bit is set to 1, accesses to the PCI configuration space are enabled. When this bit is reset to 0, accesses to the PCI configuration space are disabled.
30:24	Reserved (These bits are read only and have a value of 0).
23:16	Bus Number: Contains the bus number being targeted by the configuration cycle.
15:11	Device Number: Selects one of the 32 possible devices per bus.
10:8	Function Number: Selects one of eight possible functions within a device.
7:2	Register Number: This field selects one register within a particular bus, device, and function as specified by the other fields in the Configuration Address Register. This field is mapped to A[7:2] during HI_A-D configuration cycles.
1:0	Reserved.

5.2.2 Configuration Data Register MCH CONFIG_ADDRESS

I/O Address: 0x0CFC

Default Value: 0x0000000

Access: Read/Write

Size: 32 bits

CONFIG_DATA is a 32-bit read/write window into the PCI configuration space. The portion of configuration space that is referenced by CONFIG_DATA is determined by the contents of CONFIG_ADDRESS.

Table 42. Configuration Data Register Bit Assignments

Bit	Description
31:0	**Configuration Data Window (CDW)**: If bit 31 of CONFIG_ADDRESS is set to 1, any I/O access to the CONFIG_DATA register is mapped to configuration space pointed to by the contents of CONFIG_ADDRESS.

5.3 I/O Address Assignments

I/O port addresses are divided among the on-board devices.These devices include:

- ICH3
- ISP2312 Fibre Channel controller
- 82546 Ethernet controller
- SMSC LPC47B272 SIO
- MCH
- IPMC

Please refer to the respective device specifications for specific I/O address usage.

The MCH uses only I/O ports 0xCF8 and 0xCFC for PCI configuration cycle generation. These registers are shown in "Configuration Address Register MCH CONFIG_ADDRESS" on page 72 and "Configuration Data Register MCH CONFIG_ADDRESS" on page 73. The P64H2 forwards applicable I/O transactions to its attached PCI buses. The ISP2312 may be programmed to map its 256-byte bank of registers to memory and/or I/O space.

The I/O Address Cross-References table lists document references to I/O descriptions. Please refer to Appendix A, "Reference Documents" for a list of the referenced documents and their complete titles, revisions, and document numbers.

Table 43. I/O Address Cross-References

Device	Document Title/Number	Section/Page/Table
ICH3	ICH3 EDS	Section 7.3, Table A2 and A3
MCH	E7501 MCH EDS	Section 4.3.5 and 4.3.6
ISP2312	ISP2312 Design Guide	Section 6.6.9 and 6.7
LPC47B272	LPC47B27x Datasheet	(Throughout datasheet)
IPMC	Intel IPMC EDS	Section 4.3.7
82546	Developer's Manual, OR2941	Section 3.1.1.4

5.4 Memory Map

Table 44. Memory Map (Sheet 1 of 2)

Memory Device	Address	Size
Top of addressable memory	0xFFFF_FFFF	--
Firmware Hub Devices (x2)	0xFFE0_0000	Up to 16 Mbit
-- Firmware Hub Device 0	0xFFF0_0000	8 Mbit/1 MB
-- Firmware Hub Device 1	0xFFE0_0000	8 Mbit/1 MB
	. . .	
HI-B P64H2 IOAPIC B	0xFEC0_4000	256 bytes

Table 44. Memory Map (Sheet 2 of 2)

Memory Device	Address	Size
HI-B P64H2 IOAPIC A	0xFEC0_3000	256 bytes
HI-C P64H2 IOAPIC B	0xFEC0_2000	256 bytes
HI-C P64H2 IOAPIC A	0xFEC0_1000	256 bytes
ICH3 IOAPIC	0xFEC0_0000	256 bytes
Top of main memory …		<system dependent>
Top of Low Memory		<system dependent>
TEM-TSEG		
0100_0000	16 MB	
00F0_0000	15 MB	
0010_0000	1 MB	
FWH[1] 0/1	0xE_0000	128 KB
(PCI option ROMs, top-down allocations)		
	0xA_0000	
Main memory	0x0_0000	Up to 4 GB

NOTE: The OS may need to be recompiled to support memory above 4 Gbytes.

The Firmware Hub(s) also appears at the aliased address of (4 Gbyte – 4 Mbyte).

The MCH provides the capability to reclaim the physical memory overlapped by memory-mapped I/O devices, BIOS, and I/O APICs that reside just below 4 Gbytes. This memory may be remapped to physical memory at the address defined by the TOLM register.

5.5 IPMC Addresses

The IPMC supports 6 I^2C/SMB buses. IPMC buses 0 and 1 provide redundant IPMB connections.

The ADM1026 device is connected to SMBus 3 and provides voltage measurement capability and additional board configuration status.

Table 45. SMBus Addresses

8-bit Address (W/R)	SMBus	Description
5C/5D	3	ADM1026
A8/A9	3	SEL EEPROM

6 Specifications

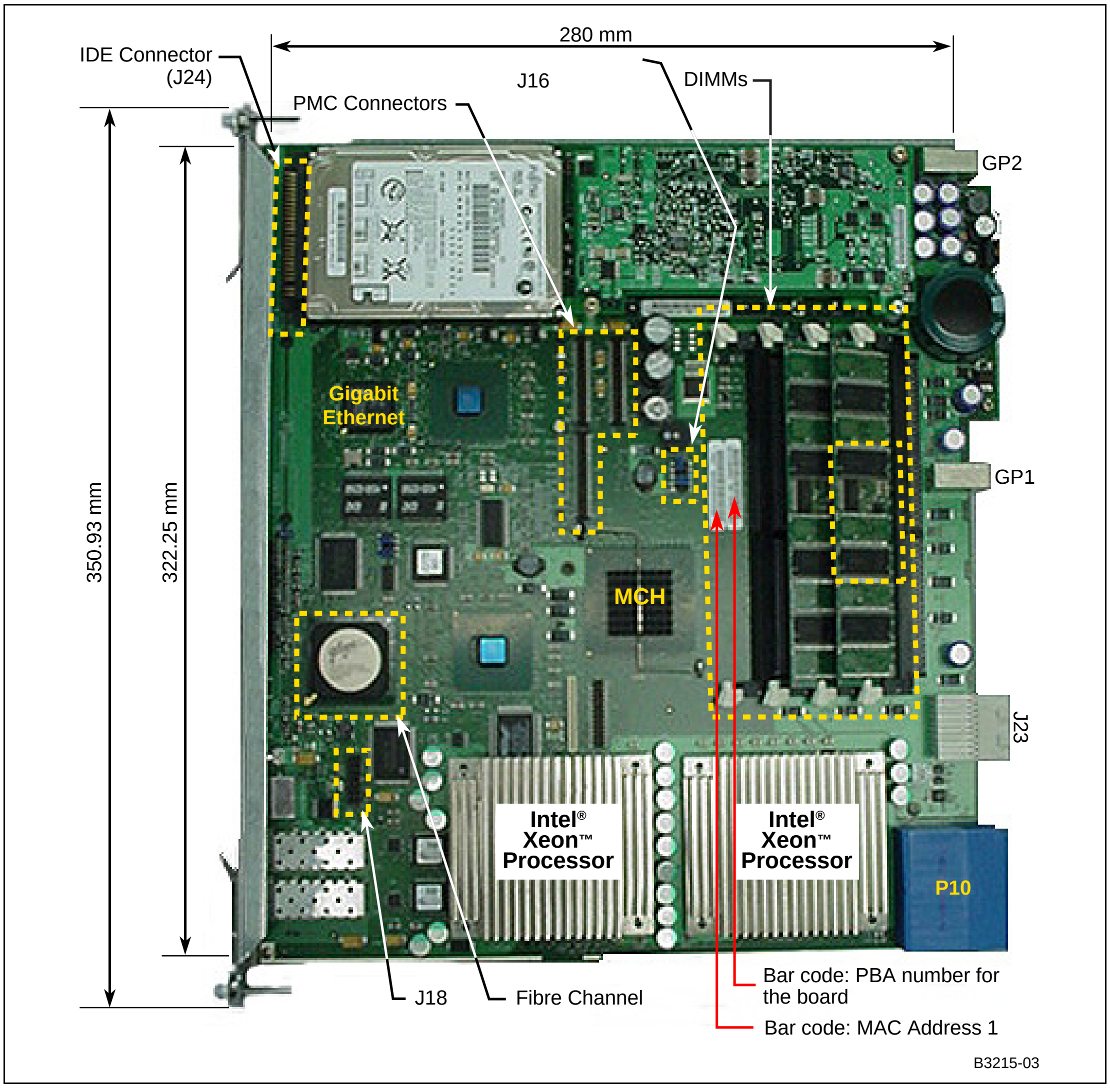
This chapter defines the AT8000 operating and nonoperating environments. It also documents the procedures followed to determine the reliability of AT8000.

6.1 Mechanical Specifications

6.1.1 Board Outline

Figure 18 is an annotated illustration of the AT8000 SBC showing the locations of major components. The board dimensions are 280 mm x 322.25 mm. The board pitch is 1.2" (30.48 mm).

Figure 18. Intel® NetStructure™ AT8000 Component Layout



NOTE: MAC Address 2 is an incremental value of MAC Address 1.

6.1.2 Backing Plate

The AT8000 SBC has a rugged metal backing plate that forms a single-piece face plate. This backing plate is made of 1.2 mm (0.048") steel which has been zinc post-plated to resist corrosion and rust. The solid backing plate provides PCB stiffening, enhanced EMI protection from adjacent boards, and protection during flame tests. The backing plate improves serviceability by making the SBC more durable.

Four holes are provided in the bottom of the backing plate for mounting an optional hard drive in the provided hard drive carrier (with the included M3 screws). Four additional holes are provided for securing an optional PMC through the front or rear standard mounting positions.

Caution: Removing the backing plate can damage the components on the board and may void the warranty. No user-serviceable parts are avilable under the PCB. Do not remove the face plate/backing plate.

6.1.3 Component Height

Figure 19, “AT8000 SBC Front Panel Dimensions – FC SKU (PMC and Connectors)” on page 79 and Figure 20, “AT8000 SBC Front Panel Dimensions – FC SKU (Screws and LEDs)” on page 80 detail maximum component heights on both the primary and secondary sides of the AT8000 SBC.

Figure 19. AT8000 SBC Front Panel Dimensions – FC SKU (PMC and Connectors)

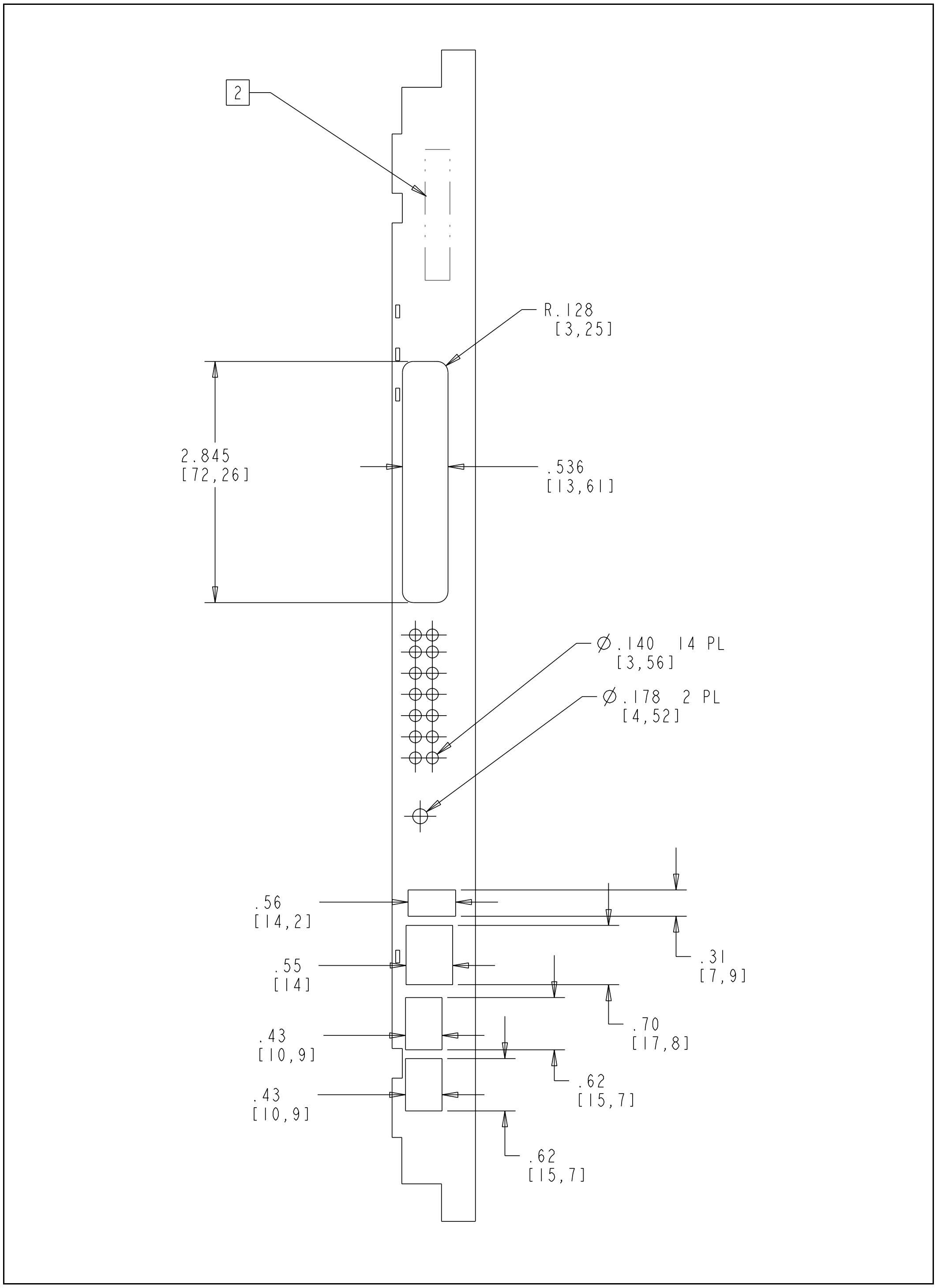


Figure 20. AT8000 SBC Front Panel Dimensions – FC SKU (Screws and LEDs)

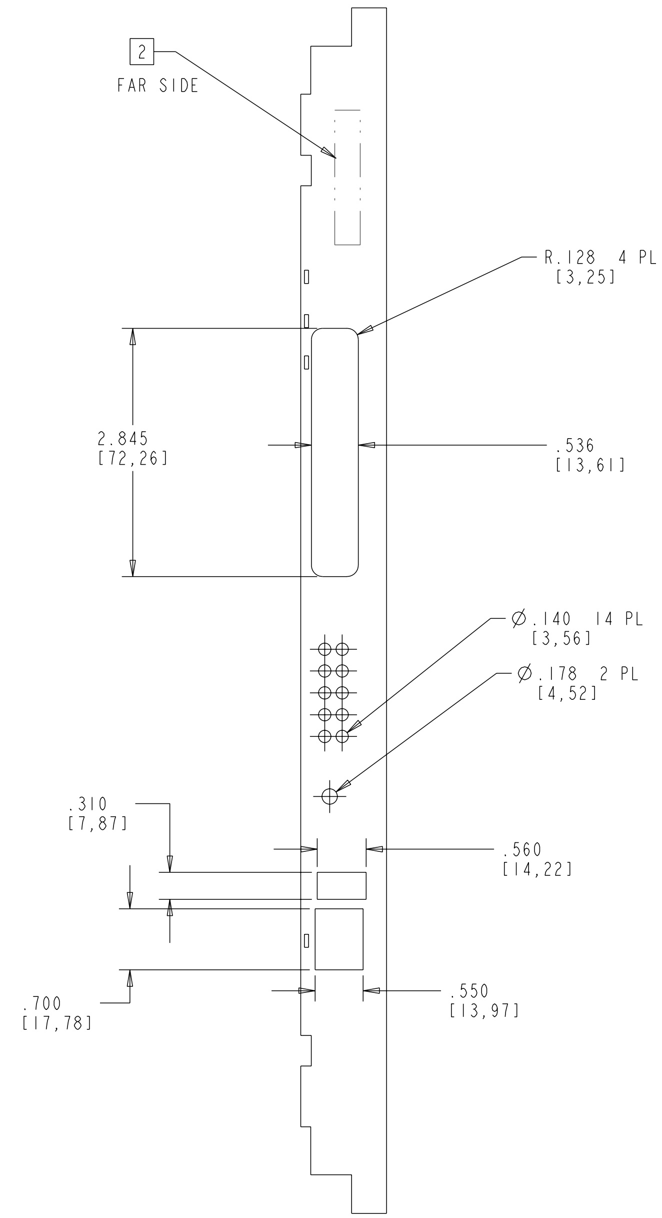


Figure 21. AT8000 SBC Front Panel Dimensions – Non FC SKU (PMC and Connectors)

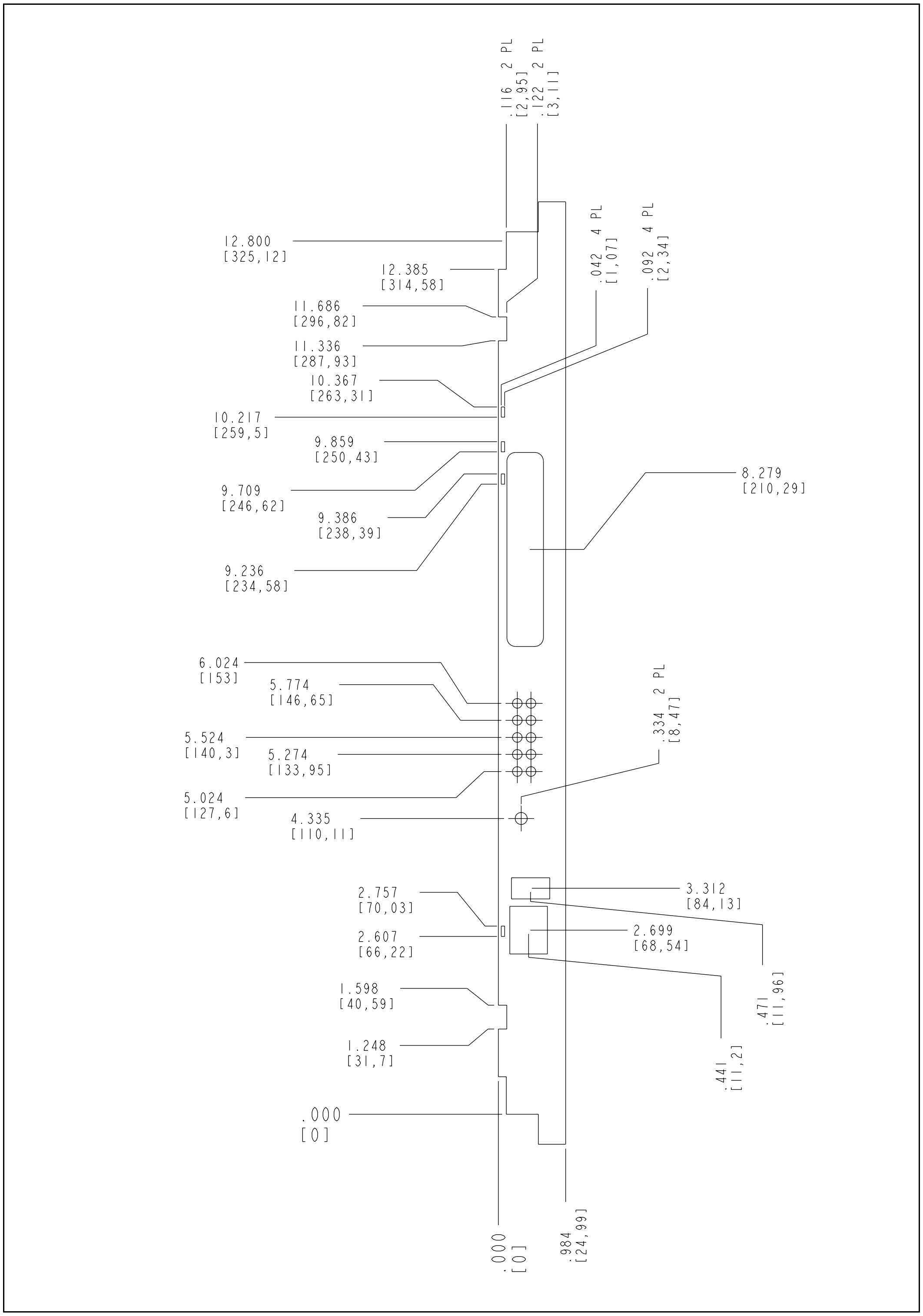
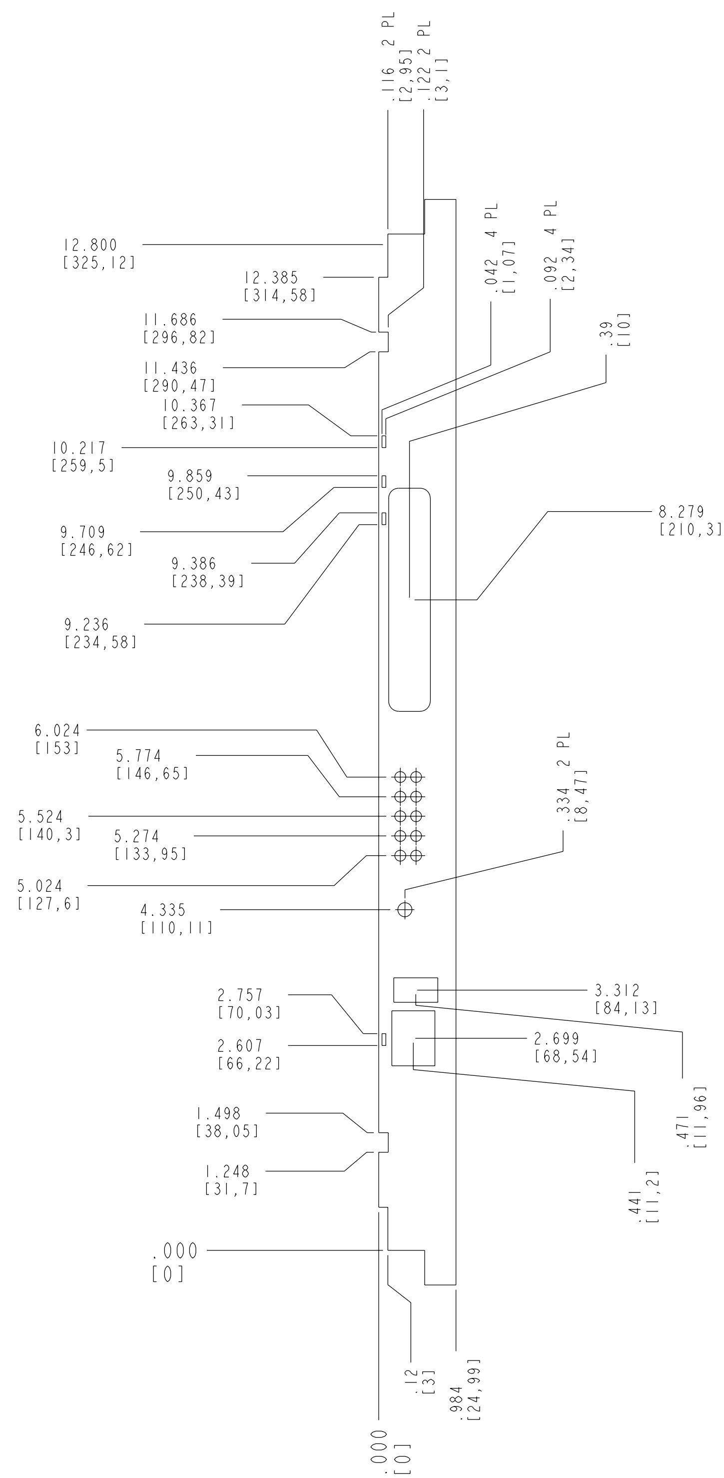


Figure 22. AT8000 SBC Front Panel Dimensions – Non-FC SKU (Screws and LED)



6.2 Environmental Specifications

The Kontron AT8000 SBC meets the board-level specifications as specified in the Intel Environmental Standards Handbook – Telco Specification Document No. A78805-01. The test methodology is a combination of Intel and NEBs test requirements with the intent that the product will pass pure system-level NEBs testing. Intel will not be completing NEBs testing on the SBC. The following table summarizes environmental limits, both operating and nonoperating.

Table 46. Environmental Specifications

Parameter	Conditions	Detailed Specification
Temperature (Ambient)	Operating	0 to 55 °C
	Storage	-40 to 70 °C
Airflow	Operating	300 linear feet per minute (LFM) minimum
Humidity	Operating	10-85% noncondensing
	Storage	10-95% noncondensing
Unpackaged Vibration	Operating	5 Hz @ 0.01 g2/Hz to 20 Hz @ 0.02g2/Hz (slope up) 20 Hz to 500 Hz @ 0.02 g2/Hz (flat) Input acceleration = 3.13 gRMS
	Storage	Not specified in current bluebook.
Shock	Unpackaged	50 g

6.3 Reliability Specifications

6.3.1 Mean Time Between Failure (MTBF) Specifications

Calculation Type: MTBF/FIT Rate

Standard: Telcordia Standard SR-332 Issue 1

Methods: Method I, Case I, Quality Level II

The calculation results were generated using the references and assumptions listed. This report and its associated calculations supersede all other released MTBF and Failure in Time (FIT) calculations of earlier report dates. The reported failure rates do not represent catastrophic failure. Catastrophic failure rates will vary based on application environment and features critical to the intended function.

Note: Incorporating an optional IDE Hard-disk Drive (HDD) will significantly impact the Reliability Specifications.

Table 47. Reliability Estimate Data

FAILURE RATE (FIT)	8,000	Failures in 10^9 hours
MTBF	125,000	Hours

6.3.1.1 Environmental Assumptions

- Failure rates are based on a 40 °C ambient temperature.
- Applied component stress levels are 50 percent (voltage, current, and/or power).
- Ground, fixed, controlled environment with an environmental adjustment factor equal to 1.0.

6.3.1.2 General Assumptions

- Component failure rates are constant.
- Board-to-system interconnects included within estimates.
- Non-electrical components (screws, mechanical latches, labels, covers, etc.) are not included within estimations.
- Printed circuit board is considered to have a 0 FIT rate.

6.3.1.3 General Notes

- Method I, Case I = Based on parts count. Equipment failure is estimated by totaling device failures rates and quantities used.
- Quality Level II = Devices purchased to specifications, qualified devices, vendor lot-to-lot controls for AQLs and DPMs.
- Where available, direct component supplier predictions or actual FIT rates have been used.
- The SBC MTBF does not include addition of the 2.5" HDD. The product MTBF could be significantly impacted by adding a HDD. Please contact the HDD manufacturer for specific component and relevant operational MTBF information.

6.3.2 Power Consumption

The power consumed by the Kontron AT8000 SBC is dependent on the type and speed of processors used and the amount of memory installed. Table 48, "Total Measured Power" on page 84 is based on the use of two Low Voltage Intel® Xeon™ processors. Typical values were obtained by running the Windows* 2000*-based application "Drive Reaper" against networked shared drives. "Max" values were obtained by running Intel's DOS* based "Maxpower" utility, version 6.0.

Note: A TriEMS card was installed for all power management tests. The TriEMS dissipates 550 mW typical.

Table 48. Total Measured Power

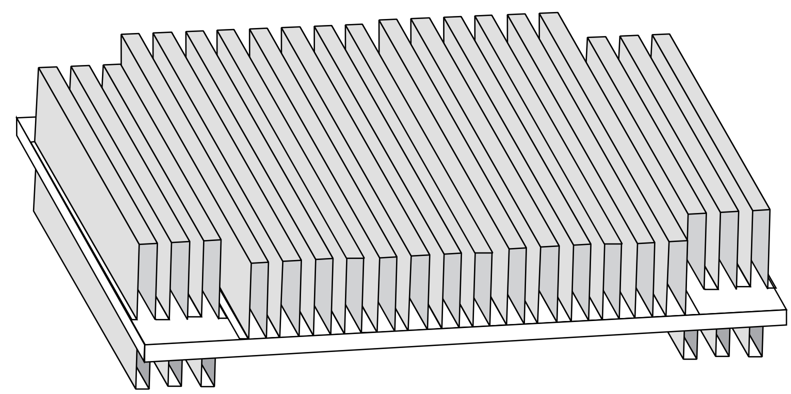
Memory	Dual 1.6 GHz (400 MHz SB)	Dual 2.0 GHz (400 MHz SB)
1 Gbyte (Two 512 Mbyte DIMMs)	110 W (typical) 132 W (max)	117 W (typical) 139 W (max)
4 Gbyte (Four 1 Gbyte DIMMs)	131 W (typical) 153 W (max)	138 W (typical) 158 W (max)

6.3.3 Cooling Requirements

The Kontron AT8000 SBC should be installed vertically in a chassis, with bottom-to-top airflow. Airflow is expected to be evenly distributed across the bottom edge of the installed AT8000 blade and maintain at least 300 LFM average airflow.

Most components on the AT8000 blade are specified to operate with a localized ambient temperature up to 70× C and do not require heat sinks. The AT8000 blade uses two custom heat sinks, one per processor (see Figure 23, “Low Voltage Intel® Xeon™ Processor Heatsink” on page 85.) The rate of airflow specified above is critical to ensuring that the blade operates as designed.

Figure 23. Low Voltage Intel® Xeon™ Processor Heatsink



6.4 Board Layer Specifications

Material: TG180 FR4

Layers: 14

Copper:

- Outer layers 1 and 14 are 1 oz copper
- Middle planes 7 & 8 are 2 oz copper
- All others are 1 oz copper.

BIOS Features 7

7.1 Introduction

The Kontron AT8000 SBC uses an Intel/AMI BIOS, which is stored in flash memory and updated using a disk-based program. In addition to the BIOS and BIOS setup program, the flash memory contains POST and Plug and Play support.

The BIOS displays a message during POST identifying the type of BIOS and a revision code. Refer to the specification update for the latest default settings.

7.2 BIOS Flash Memory Organization

AT8000 contains two Firm Ware Hub (FWH) devices (see Figure 1, "AT8000 SBC Block Diagram" on page 14). The first one is the Primary FWH, which holds the BIOS code that executes during POST. The second is the Backup FWH, which recovers the system when the Primary FWH is corrupted. The N82802AC FWH includes an 8 Mbit (1024 KByte) symmetrical flash memory device. Internally, the device is grouped into sixteen 64-KByte blocks that are individually erasable, lockable, and unlockable.

7.3 Complementary Metal-Oxide Semiconductor (CMOS)

CMOS RAM is a nonvolatile storage that stores data needed by the BIOS. The data consists of certain onboard configurable settings, including time and date. CMOS resides in the ICH3 and is powered by the Supercap when the blade is power off. The settings in the BIOS setup menu are stored in the CMOS RAM and are often called CMOS settings.

7.3.1 Copying and Saving CMOS Settings

The BIOS/CMOS flash update utility (flashlnx or flashdos) loads a fresh copy of the BIOS into flash ROM. It has the capability to save the CMOS settings from the AT8000 SBC. The CMOS settings file can be copied to a file. This file can be saved in a directory specified by the user. The filename also can be specified by user, such as CMOS.BIN.

With the BIOS/CMOS flash utility and CMOS.bin file, user is able to copy CMOS settings to another AT8000 SBC, thus minimizing the effort to reconfigure the preferred CMOS settings across all boards.

This BIOS/CMOS flash utility that is designed to run under MontaVista* Carrier Grade Linux* 3.0 should be on the local hard disk of the AT8000. Any user who is able to communicate with the AT8000 via Telnet would be able to execute to copy and save the CMOS remotely.

The utility is part of the BIOS release package and can be downloaded from the Intel web site at http://www.intel.com/ design/network/products/cbp/atca/index.htm. Refer to Chapter 10, "Operating the Unit," for more information.

7.4 Redundant BIOS Functionality

AT8000 hardware has two flash banks for BIOS where redundant copies are stored. BIOS bank selection logic is connected to the IPMC, and the IPMC firmware allows selection of the BIOS bank.

By default, firmware selects BIOS bank 0. BIOS executes code off this flash and performs checksum validation of its operational code. This checksum occurs in the boot block of the BIOS. If the boot block detects a checksum failure in the remainder of the BIOS, it notifies the IPMC of the failure. In case of failure, the IPMC firmware:

1. Asserts the RESET pin on the processor.
2. Switches the flash bank.
3. Deasserts the RESET pin on the processor, allowing BIOS to execute off the second flash bank.

7.5 System Management BIOS (SMBIOS)

SMBIOS is a Desktop Management Interface-compliant method for managing computers in a managed network.

The main component of SMBIOS is the management information format database, which contains information about the computing system and its components. Using SMBIOS, a system administrator can obtain the following information for system components:

- System types.
- Capabilities.
- Operational status.
- Installation dates.

The management information format database defines the data and provides the method for accessing this information. The BIOS enables applications such as third-party management software to use SMBIOS. The BIOS stores and reports the following SMBIOS information:

- BIOS data, such as the BIOS revision level.
- Fixed-system data, such as peripherals, serial numbers, and asset tags.
- Resource data, such as memory size, cache size, and processor speed.

Non-Plug and Play operating systems, such as Linux or Windows NT*, require an additional interface for obtaining the SMBIOS information. The BIOS supports an SMBIOS table interface for such operating systems. Using this support, an SMBIOS service-level application running on a non-Plug and Play operating system can obtain the SMBIOS information.

7.6 Legacy USB Support

Legacy USB support enables USB devices such as keyboards, mice, and hubs to be used even when the operating system's USB drivers are not yet available. Legacy USB support is used to access the BIOS Setup program and install an operating system that supports USB. Legacy USB support is set to Enabled by default.

Note: Legacy USB support is for keyboards, mice and hubs only. Other USB devices are not supported in legacy mode except bootable devices like CD-ROM drives and floppy disk drives.

Legacy USB support operates as follows:

1. When you apply power to the computer, legacy support is disabled.
2. POST begins.
3. Legacy USB support is enabled by the BIOS, allowing you to use a USB keyboard.
4. POST completes.
5. The operating system loads. USB keyboards and mice are recognized and may be used to configure the operating system. Keyboards and mice are not recognized during this period if Legacy USB support was set to Disabled in the BIOS Setup program.
6. After the operating system loads the USB drivers, all legacy and non-legacy USB devices are recognized by the operating system. Legacy USB support from the BIOS is no longer used.

To install an operating system that supports USB, verify that Legacy USB support in the BIOS Setup program is set to Enabled and follow the operating system's installation instructions.

7.7 BIOS Updates

The BIOS can be updated using either of the following utilities, which are available on the Intel Web site:

- Intel® Linux* BIOS Update utility, which enables automated updating while in the Linux environment. Using this utility, the BIOS can be updated from:
  - A file on a hard disk
  - 1.44 MByte diskette
  - CD-ROM
  - The file location on the Web
- Intel® DOS* BIOS Update utility, which enables automated updating while in the DOS environment.

Both utilities support the following BIOS maintenance functions:

- Updating the main BIOS.
- Verifying that the updated BIOS matches the target system to prevent accidentally installing an incompatible BIOS.

Refer to Chapter 10, "BIOS Image Updates," for a complete upgrade procedure.

Note: Review the instructions distributed with the upgrade utility before attempting a BIOS update.

7.7.1 Language Support

English is the only supported language.

7.8 Recovering BIOS Data

Some types of failure can destroy the BIOS. For example, the data can be lost if a power outage occurs while the BIOS is being updated in flash memory. The BIOS can be recovered from Backup BIOS. Recovery mode is active when BIOS checksum fails and notifies the IPMC to failover to the backup BIOS.

7.9 Boot Options

In the BIOS Setup program, the user can choose to boot from available boot devices, with each boot device having options for removable media, CD-ROM, hard drive, IBA2, or IBA1. In every POST, the BIOS detects all available boot devices, then displays them on the boot order screen, with the exception of the IBA, which displays even if the LAN cable is not connected.

The default settings are:

- 1st Boot Device: removable media
- 2nd Boot Device: CD-ROM
- 3rd Boot Device: hard drive
- 4th Boot Device: IBA2 - Intel® Boot Agent (IBA) 2
- 5th Boot Device: IBA1 - Intel® Boot Agent (IBA) 1

7.9.1 CD-ROM and Network Boot

Booting from CD-ROM is supported in compliance with the El Torito bootable CD-ROM format specification. Under the Boot menu in the BIOS Setup program, USB CD-ROM is listed as a boot device (removable media). Boot devices are defined in priority order.

Accordingly, if there is not a bootable CD in the CD-ROM drive, the system attempts to boot from the next defined drive.

The network can be selected as a boot device. This Intel® Boot Agent (IBA) selection allows booting from the onboard LANs if connected to a network. Typically, AT8000's Gigabit Ethernet is routed through the ATCA backplane to the front panel of an ATCA switch, which is then connected to a LAN.

7.9.2 Booting without Attached Devices

For use in embedded applications, the BIOS has been designed so that after passing the POST, the operating system loader is invoked even if the video adapter (via PMC), keyboard, or mouse are not present:

7.10 Fast Booting Systems

7.10.1 Quick Boot

Use of the following BIOS Setup program settings reduces the POST execution time.

In the Boot Menu:

- Disable Option - ROM(s) if customer configuration does not use IBA(PXE) boot, or there is no FibreChannel drive in the system.
- Disable Quiet Boot eliminates display of the logo splash screen. This could save several seconds of painting complex graphic images and changing video modes.
- Enable Quick Boot bypasses memory count and the search for a removable drive.

Note: It is possible to optimize the boot process to the point where the system boots so quickly that the Intel logo screen (or a custom logo splash screen, if implemented) is be seen. Monitors and hard disk drives with minimum initialization times can also contribute to a boot time that might be so fast that necessary logo screens and POST messages cannot be seen.

Note: This boot time may be so fast that some drives might be not be initialized at all. If this occurs, it is possible to introduce a programmable delay ranging from 3 to 30 seconds using the BIOS Setup program, IDE Configuration Submenu, Advanced Menu, IEDE Detect Time Out feature.

7.11 BIOS Security Features

The BIOS includes security features that restrict access to the BIOS Setup program and booting the computer. A supervisor password and a user password can be set for the BIOS Setup program and for booting the computer, with the following restrictions:

- The supervisor password gives unrestricted access to view and change all the Setup options in the BIOS Setup program. This is the supervisor mode.
- The user password gives restricted access to view and change Setup options in the BIOS Setup program. This is the user mode.
- If only the supervisor password is set, pressing the <Enter> key at the password prompt of the BIOS Setup program allows the user restricted access to Setup.
- If both the supervisor and user passwords are set, users can enter either the supervisor password or the user password to access Setup. Users have access to Setup respective to which password is entered.
- Setting the user password restricts who can boot the computer. The password prompt is displayed before the computer is booted. If only the supervisor password is set, the computer boots without asking for a password. If both passwords are set, the user can enter either password to boot the computer.

The table below shows the effects of setting the supervisor password and user password. This table is for reference only and is not displayed on the screen.

Table 49. Supervisor and User Password Functions

Password Set	Supervisor Mode	User Mode	Password to Enter Setup	Password During Boot
None	Any user can change all options	Any user can change all options	None	None
Supervisor and user	Can change all options	Based on user access level: No Access, View Only, Limited, Full Access	Supervisor or user	If password check option is set to Setup then no password required. Otherwise requires either supervisor or user password.
Supervisor only	Can change all options	Based on user access level: No Access, View Only, Limited, Full Access.	Supervisor (for supervisor mode) or enter only (for user mode)	If password check option is set to Setup then no password required. Otherwise requires either supervisor password or enter only.
User only	Can't get into supervisor mode until user pass-word is cleared.	Can change all options	User	If password check option is set to Setup then no password required. Otherwise requires user password.

7.12 Remote Access Configuration

Remote access using serial console redirection allows users to monitor the AT8000 boot process and run the AT8000 BIOS setup from a remote serial terminal. Connection is made directly through a serial port.

The console redirection feature is useful in cases where it is necessary to communicate with a processor board in an embedded application without video support.

Table 50 shows the escape code sequences that may be useful for things like BIOS Setup if function keys cannot be directly sent from a terminal application:

Table 50. Function Key Escape Code Equivalents

Key	Escape Sequence	Note
F1	ESC OP	
F2	ESC OQ	
F3	ESC OR	
F4	ESC OS	To enter BIOS Setup
F5	ESC OT	
F6	ESC OU	
F7	ESC OV	
F8	ESC OW	
F9	ESC OX	
F10	ESC OY	To save and exit Setup
F11	ESC OZ	
F12	ESC OI	PXE boot

Error Messages 8

8.1 BIOS Error Messages

The following table lists the error messages.

Table 51. BIOS Error Messages

Error Message
Timer count read/write error
CMOS battery error
CMOS diagnostic status error
CMOS checksum error
CMOS memory size error
RAM read/write test error
Floppy disk drive 0 error
Floppy disk drive 1 error
Floppy controller error
CMOS date/time error
Clear CMOS jumper error
Clear Password jumper error
Manufacturing jumper error
BMC in Update error
BMC Response Fail error
Event Log Full error

8.2 Port 80h POST Codes

During the POST, the BIOS generates diagnostic progress codes (POST-codes) to I/O port 80h. If the POST fails, execution stops and the last POST code generated is left at port 80h. This code is useful for determining the point where an error occurred.

Displaying the POST codes requires an add-in card, often called a POST card (PCI, not ISA). The POST card decodes the port and displays the contents on a medium such as a seven-segment display.

Table 53, Table 54, and Table 55 offer descriptions of the POST codes generated by the BIOS. They define the uncompressed INIT code checkpoints, the boot block recovery code checkpoints, and the runtime code uncompressed in F000 shadow RAM.

Note: Some codes are repeated in the tables because they apply to more than one operation.

Table 52. Bootblock Initialization Code Checkpoints

Checkpoint	Description
Before D1	Early chipset initialization is done. Early super I/O initialization is done, including RTC and keyboard controller. NMI is disabled.
D1	Perform keyboard controller BAT test. Check if waking up from power management suspend state. Save power-on CPUID value in scratch CMOS.
D0	Go to flat mode with 4 GByte limit and GA20 enabled. Verify the bootblock checksum.
D2	Disable CACHE before memory detection. Execute full memory sizing module. Verify that flat mode is enabled.
D3	If memory sizing module not executed, start memory refresh and do memory sizing in Bootblock code. Do additional chipset initialization. Re-enable CACHE. Verify that flat mode is enabled.
D4	Test base 512 KByte memory. Adjust policies and cache first 8 GBytes. Set stack.
D5	Bootblock code is copied from ROM to lower system memory and control is given to it. BIOS now executes out of RAM.
D6	Both key sequence and OEM-specific methods are checked to determine if BIOS recovery is forced. Main BIOS checksum is tested. If BIOS recovery is necessary, control flows to checkpoint E0.
D7	Restore CPUID value back into register. The Bootblock-Runtime interface module is moved to system memory and control is given to it. Determine whether to execute serial flash.
D8	The Runtime module is uncompressed into memory. CPUID information is stored in memory.
D9	Store the Uncompressed pointer for future use in PMM. Copying Main BIOS into memory. Leaves all RAM below 1 MByte Read-Write including E000 and F000 shadow areas but closing SMRAM.
DA	Restore CPUID value back into register. Give control to BIOS POST (ExecutePOSTKernel). See Table 53, “POST Code Checkpoints” on page 94 for more information.

Table 53. POST Code Checkpoints (Sheet 1 of 3)

Checkpoint	Description
03	Disable NMI, parity, video for EGA, and DMA controllers. Initialize BIOS, POST, runtime data area. Also initialize BIOS modules on POST entry and GPNV area. Initialized CMOS as mentioned in the kernel variable.
	Check CMOS diagnostic byte to determine if battery power is OK and CMOS checksum is OK. Verify CMOS checksum manually by reading storage area. If the CMOS checksum is bad, update CMOS with power-on default values and clear passwords. Initialize status register A. Initializes data variables that are based on CMOS setup questions. Initializes both the 8259 compatible PICs in the system.
05	Initializes the interrupt controlling hardware (generally PIC) and interrupt vector table.
06	Do R/W test to CH-2 count reg. Initialize CH-0 as system timer. Install the POSTINT1Ch handler. Enable IRQ-0 in PIC for system timer interrupt. Traps INT1Ch vector to "POSTINT1ChHandlerBlock."
08	Initializes the CPU. The BAT test is being done on KBC. Program the keyboard controller command byte is being done after Auto detection of KB/MS using AMI KB-5.
C0	Early CPU Init Start -- Disable Cache - Init Local APIC.
C1	Set up bootstrap processor Information.
C2	Set up bootstrap processor for POST.
C5	Enumerate and set up application predecessors.

Table 53. POST Code Checkpoints (Sheet 2 of 3)

Checkpoint	Description
C6	Re-enable cache for bootstrap processor.
C7	Early CPU Init Exit.
0A	Initializes the 8042-compatible Keyboard Controller.
0B	Detects the presence of PS/2 mouse.
0C	Detects the presence of Keyboard in KBC port.
0E	Testing and initialization of different Input Devices. Also, update the Kernel Variables. Traps the INT09h vector, so that the POST INT09h handler gets control for IRQ1. Uncompress all available language, BIOS logo, and Silent logo modules.
13	Early POST initialization of chipset registers.
24	Uncompress and initialize any platform specific BIOS modules.
30	Initialize System Management Interrupt.
2A	Initializes different devices through DIM. See Table 54, “DIM Code Checkpoints” on page 96 for more information.
2C	Initializes different devices. Detects and initializes the video adapter installed in the system that have optional ROMs.
2E	Initializes all the output devices.
31	Allocate memory for ADM module and uncompress it. Give control to ADM module for initialization. Initialize language and font modules for ADM. Activate ADM module.
33	Initializes the silent boot module. Set the window for displaying text information.
37	Displaying sign-on message, CPU information, setup key message, and any OEM-specific information.
38	Initializes different devices through DIM. See Table 54, “DIM Code Checkpoints” on page 96 for more information.
39	Initializes DMAC-1 & DMAC-2.
3A	Initialize RTC date/time.
3B	Test for total memory installed in the system. Also, check for DEL or ESC keys to limit memory test. Display total memory in the system.
3C	Mid POST initialization of chipset registers.
40	Detect different devices (Parallel ports, serial ports, and coprocessor in CPU, etc.) successfully installed in the system and update the BDA, EBDA, etc.
50	Programming the memory hole or any kind of implementation that needs an adjustment in system RAM size if needed.
52	Updates CMOS memory size from memory found in memory test. Allocates memory for Extended BIOS Data Area from base memory.
60	Initializes NUM-LOCK status and programs the KBD typematic rate.
75	Initialize Int-13 and prepare for IPL detection.
78	Initializes IPL devices controlled by BIOS and option ROMs.
7A	Initializes remaining option ROMs.
7C	Generate and write contents of ESCD in NVRam.
84	Log errors encountered during POST.
85	Display errors to the user and gets the user response for error.
87	Execute BIOS setup if needed.

Table 53. POST Code Checkpoints (Sheet 3 of 3)

Checkpoint	Description
8C	Late POST initialization of chipset registers.
8D	Build ACPI tables (if ACPI is supported).
8E	Program the peripheral parameters. Enable/Disable NMI as selected.
90	Late POST initialization of system management interrupt.
A0	Check boot password if installed.
A1	Clean-up work needed before booting to OS.
A2	Takes care of runtime image preparation for different BIOS modules. Fill the free area in F000h segment with 0FFh. Initializes the Microsoft IRQ Routing Table. Prepares the runtime language module. Disables the system configuration display if needed.
A4	Initialize runtime language module.
A7	Displays the system configuration screen if enabled. Initialize the CPUs before boot, which includes the programming of the MTRRs.
A8	Prepares CPU for OS boot, including final MTRR values.
A9	Waits for user input at config display if needed.
AA	Uninstalls POST INT1Ch vector and INT09h vector. Deinitializes the ADM module.
AB	Prepares BBS for Int 19 boot.
AC	End of POST initialization of chipset registers.
B1	Saves system context for ACPI.
00	Passes control to OS Loader (typically INT19h).

Table 54. DIM Code Checkpoints

Checkpoint	Description
2A	Initializes different buses and performs the following functions: • **Function 0: Reset, Detect, and Disable** - Disables all device nodes, PCI devices, and PnP ISA cards. Assigns PCI bus numbers. • **Function 1: Static Device Initialization** - initializes all static devices that include manual configured onboard peripherals, memory and I/O decode windows in PCI-PCI bridges, and noncompliant PCI devices. Reserves static resources. • **Function 2: Boot Output Device Initialization** - Searches for and initializes any PnP, PCI, or AGP video devices.
38	Initializes different buses and performs the following functions: • **Function 3: Boot Input Device Initialization** - Searches for and configures PCI input devices and detects if system has standard keyboard controller. • **Function 4: IPL Device Initialization** - searches for and configures all PnP and PCI boot devices. • **Function 5: General Device Initialization** - Configures all onboard peripherals that are set to automatic configuration and configures all remaining PnP and PCI devices.

Table 55. ACPI Runtime Checkpoints

Checkpoint	Description
AC	First ASL check point. Indicates the system is running in ACPI mode.
AA	System is running in APIC mode.
01, 02, 03, 04, 05	Entering sleep state S1, S2, S3, S4, or S5.
10, 20, 30, 40, 50	Waking from sleep state S1, S2, S3, S4, or S5.

The following table describes the beep codes implemented in the AT8000 BIOS.

Table 56. BIOS Beep Codes

Number of Beeps	Description
1	Memory refresh timer error
3	Main memory read/write test error
6	Keyboard controller BAT test error
8	Display Memory error

BIOS Setup 9

9.1 Introduction

The BIOS Setup program can be used to view and change the BIOS settings for the computer. The BIOS Setup program is accessed by pressing the <F2> key after the Power-On Self-Test (POST) begins and before the operating system boot begins. Table 57 lists the BIOS Setup program menu features.

Table 57. BIOS Setup Program Menu Bar

Main	Advanced	Boot	Security	Exit
Allocates resources for hardware components	Configures advanced features available through the chipset	Selects boot options and power supply controls	Sets passwords and security features	Saves or discards changes to Setup program options

Table 58 lists the function keys available for menu screens.

Table 58. BIOS Setup Program Function Keys

BIOS Setup Program Function Key	Description
<←> or <→>	Selects a different menu screen (moves the cursor left or right).
<↑> or <↓>	Selects an item (moves the cursor up or down).
<Tab>	Selects a field (not implemented).
<Enter>	Executes command or selects the submenu.
<F9>	Loads the default configuration values for the current menu.
<F10>	Saves the current values and exits the BIOS Setup program.
<Esc>	Exits the menu.

9.2 Main Menu

To access this menu, select Main on the menu bar at the top of the screen.

Main	Advanced	Boot	Security	Exit

Table 59 describes the Main menu. This menu reports processor and memory information and is used for configuring the system date and system time.

Table 59. Main Menu

Feature	Options	Description
BIOS ID	AMIBIOS Version Build Date ID	Displays the BIOS ID.
Processor	Type Speed Count	Reports processor type, speed, CPUID and L2 Cache size.
System Memory Size	Size	Displays system memory size.
System Time	Hour, minute, and second	Specifies the current time.
System Date	Day of week Month/day/year	Specifies the current date.

9.3 Advanced Menu

To access this menu, select Advanced on the menu bar at the top of the screen.

Main	Advanced	Boot	Security	Exit
`CPU Configuration`				
`IDE Configuration`				
`SuperIO Configuration`				
`ACPI Configuration`				
`System Management Configuration`				
`Event Logging Configuration`				
`Fibre Channel Routing (PICMG)`				
`Remote Access Configuration`				
`USB Configuration`				
`PCI Configuration`				

Under the Advanced Menu, the following warning message appears:

WARNING: Setting the wrong values in the sections that follow may cause the system to malfunction.

This is a warning message to users to not modify the settings unless they are familiar with the items. To restore factory defaults, go to "Exit > Load Optimal Defaults".

Table 60 describes the Advanced menu. This menu sets advanced features that are available through the chipset.

Table 60. Advanced Menu

Feature	Options	Description
CPU Configuration	Select to display submenu	Display CPU details, Enable/Disable Hyper-Threading technology.
IDE Configuration	Select to display submenu	Display the primary IDE master and primary IDE slave drive.
SuperIO Configuration	Select to display submenu	Set the serial port 1 address/interrupt.
ACPI Configuration	Select to display submenu	Enable/Disable ACPI support for OS, Enable/Disable additional ACPI 2.0 tables.
System Management Configuration	Select to display submenu	Display FRU board and product information, Display BMC device and FW information.
Event Logging Configuration	Select to display submenu	Enable/Disable error logging.
Fibre Channel Routing (PICMG)	Select to display submenu	Select Fibre Channel connections.
Remote Access Configuration	Select to display submenu	Set remote access type, set serial port settings, Enable/Disable redirection after booting to DOS.
USB Configuration	Select to display submenu	Enable/Disable USB devices.
PCI Configuration	Select to display submenu	Enable/Disable onboard Fibre Channel option.

9.3.1 CPU Configuration Submenu

To access this submenu, select Advanced on the menu bar, then CPU Configuration.

Main	Advanced	Boot	Security	Exit
CPU Configuration				
Manufacturer				
Brand String				
Frequency				
HyperThreading				

The submenu represented in the following table is used for configuring the CPU.

Table 61. CPU Configuration Submenu

Feature	Options	Description
Manufacturer		Display CPU Manufacturer
Brand String		Display CPU Brand String
Frequency		Display CPU Frequency
HyperThreading	Disabled **Enabled**	Enable/Disable Hyper-Threading Technology.

NOTE: **Bold** text indicates default setting.

9.3.2 IDE Configuration Submenu

To access this submenu, select Advanced on the menu bar, then IDE Configuration.

Main	Advanced	Boot	Security	Exit
CPU Configuration				
IDE Configuration				
Primary IDE Master/Slave				
Floppy Configuration				
SuperIO Configuration				
ACPI Configuration				
Advanced ACPI Configuration				
System Management Configuration				
Event Logging Configuration				
Fibre Channel Routing (PICMG)				
Remote Access Configuration				
USB Configuration				
PCI Configuration				

Table 62 shows IDE device configuration options.

Table 62. IDE Configuration Submenu (Sheet 1 of 2)

Feature	Options	Description
On Board PCI IDE Controller	Disabled **Primary**	Enable/Disable on board Primary IDE Controller.Disabled: disables the integrated IDE Controller.Primary: enables only the Primary IDE Controller.
Primary IDE Master		Display the primary IDE master drive.While entering setup, BIOS auto detects the presence of IDE devices. This displays the status of the auto detection of IDE devices.
Primary IDE Slave		Display the primary IDE slave drive.While entering setup, BIOS auto detects the presence of IDE devices. This displays the status of the auto detection of IDE devices.

Table 62. IDE Configuration Submenu (Sheet 2 of 2)

Feature	Options	Description
Hard Disk Write Protect	**Disabled** Enabled	Enable/Disable Hard Disk device write protection. This is effective only if the device is accessed through BIOS.
IDE Detect Time Out	0 5 10 15 20 25 30 **35**	Select the time out value for detecting ATA/ATAPI device(s).
ATA(PI) 80Pin Cable Detect.	**Host&Device** Host	Select the mechanism for detecting 80Pin ATA(PI) Cable.

NOTE: **Bold** text indicates default setting.

9.3.2.1 Primary IDE Master/Slave Submenu

Main	Advanced	Boot	Security	Exit

`CPU Configuration`
`IDE Configuration`
`Primary IDE Master/Slave`
`Floppy Configuration`
`SuperIO Configuration`
`ACPI Configuration`
`System Management Configuration`
`Event Logging Configuration`
`Fibre Channel Routing (PICMG)`
`Remote Access Configuration`
`USB Configuration`
`PCI Configuration`

Table 63. Primary IDE Master/Slave Submenu

Feature	Options	Description
Device		Display IDE device.
Vendor		Display IDE vendor name.
Size		Display IDE device size.
LBA Mode		Display IDE LBA Mode status.
Block Mode		Display IDE Block Mode status.
PIO Mode		Display PIO Mode status.
Async DMA		Display Async DMA status.
Ultra DMA		Display Ultra DMA-5 status.
S.M.A.R.T		Display S.M.A.R.T status.
Type	Not installed **Auto** CDROM ARMD	Select the type of IDE device connected.
LBA/Large Mode	Disabled **Auto**	Disable: Disable LBA ModeAuto: Enable the LBA Mode if the device supports it and the devices is not already formatted with LBA Mode disable.
Block (Multi-Sector Transfer)	Disabled **Auto**	Disable: The data transfer from and to the device occurs one sector at a time. Auto: The data transfer from and to the device occurs multiple sectors at a time if the device supports it.
PIO Mode	**Auto** 0/1/2/3/4	Select PIO Mode
DMA Mode	**Auto** SWDMA0 SWDMA1 SWDMA2 MWDMA0 MWDMA1 MWDMA2 UDMA0 UDMA1 UDMA2 UDMA3 UDMA4	Select DMA Mode Auto: Auto detected SWDMAn: SingleWordDMAn MWDMAn: MultiWordDMAn UDMAn: UltraDMAn
S.M.A.R.T	**Auto** Disabled Enabled	Enable/Disable S.M.A.R.T. Auto: Enable S.M.A.R.T if the device supports it.
32 Data Transfer	**Disabled** Enabled	Enable/Disable 32-bit Data Transfer.
ARMD Emulation Type	**Auto** FloppyHard Disk	Select ARMD device emulation type by BIOS.

NOTE: **Bold** text indicates default setting.

9.3.3 Floppy Configuration Submenu

To access this submenu, select Advanced on the menu bar, then Floppy Configuration.

Main	Advanced	Boot	Security	Exit
CPU Configuration				
IDE Configuration				
Floppy Configuration				
SuperIO Configuration				
ACPI Configuration				
System Management Configuration				
Event Logging Configuration				
Fibre Channel Routing (PICMG)				
Remote Access Configuration				
USB Configuration				
PCI Configuration				

Table 64 shows floppy device configuration options.

Table 64. Floppy Configuration Submenu

Feature	Options	Description
Floppy A	**Disabled** 360 KByte 1.2 MByte 720 KByte 1.44 MByte 2.88 MByte	Set the floppy A type.

NOTE: **Bold** text indicates default setting.

9.3.4 SuperIO Configuration Submenu

To access this submenu, select Advanced on the menu bar, then SuperIO Configuration.

Main	Advanced	Boot	Security	Exit
CPU Configuration				
IDE Configuration				
Floppy Configuration				
SuperIO Configuration				
ACPI Configuration				
System Management Configuration				
Event Logging Configuration				
Fibre Channel Routing (PICMG)				
Remote Access Configuration				
USB Configuration				
PCI Configuration				

Table 65 shows SuperIO configuration options.

Table 65. SuperIO Configuration Submenu

Feature	Options	Description
OnBoard Floppy Controller	**Disabled** Enabled	Enable or disable Floppy Controller.
Serial Port1 Address	Disabled **3F8/IRQ4** 2F8/IRQ3 3E8/IRQ4 2E8/IRQ3	Set the serial port 1 address/interrupt.

NOTE: Bold text indicates default setting.

9.3.5 ACPI Configuration Submenu

To access this submenu, select Advanced on the menu bar, then ACPI Configuration.

Main	Advanced	Boot	Security	Exit
`CPU Configuration`				
`IDE Configuration`				
`Floppy Configuration`				
`SuperIO Configuration`				
`ACPI Configuration`				
`Advanced ACPI Configuration`				
`System Management Configuration`				
`Event Logging Configuration`				
`Fibre Channel Routing (PICMG)`				
`Remote Access Configuration`				
`USB Configuration`				
`PCI Configuration`				

Table 66 shows ACPI configuration options.

Table 66. ACPI Configuration Submenu

Feature	Options	Description
ACPI Aware O/S	No **Yes**	Enable/Disable ACPI support for OS. Enable: If OS supports ACPI. Disable: If OS does not support ACPI.

NOTE: **Bold** text indicates default setting.

9.3.5.1 Advanced ACPI Configuration Submenu

To access this submenu, select Advanced on the menu bar, then ACPI Configuration.

Main	Advanced	Boot	Security	Exit
`CPU Configuration`				
`IDE Configuration`				
`Floppy Configuration`				
`SuperIO Configuration`				
`ACPI Configuration`				
`Advanced ACPI Configuration`				
`System Management Configuration`				
`Event Logging Configuration`				
`Fibre Channel Routing (PICMG)`				

Remote Access Configuration
USB Configuration
PCI Configuration

Table 67 shows ACPI configuration options.

Table 67. Advanced ACPI Configuration Submenu

Feature	Options	Description
ACPI 2.0 Support	**No** Yes	Add additional ACPI 2.0 tables as per ACPI2.0 specifications.
ACPI APIC support	Disabled **Enabled**	Include ACPI APIC table pointer to RSDT pointer list.
BIOS→AML ACPI table	Disabled **Enabled**	Include BIOS→AML exchange table pointer to (X)RSDT pointer list.
Headless Mode	**Disabled** Enabled	Enable/Disable Headless operation mode through ACPI.

NOTE: Bold text indicates default setting.

9.3.6 System Management Configuration Submenu

To access this submenu, select Advanced on the menu bar, then System Management Configuration.

Main	Advanced	Boot	Security	Exit
CPU Configuration				
IDE Configuration				
Floppy Configuration				
SuperIO Configuration				
ACPI Configuration				
System Management Configuration				
Event Logging Configuration				
Fibre Channel Routing (PICMG)				
Remote Access Configuration				
USB Configuration				
PCI Configuration				

Table 68 shows System Management configuration options.

Table 68. System Management Configuration Submenu

Feature	Options	Description
FRU Board Information Area		Display FRU Board Information.
Board Product Name		
Board Serial Number		

Table 68. **System Management Configuration Submenu**

Board Part Number		
FRU Product Information Area		Display FRU Product Information.
Product Name		
Product Part/Model		
Product Version Number		
Product Serial Number		
BMC Device and FW Information		Display BMC Device and FW Information.
BMC Device ID		
BMC Firmware Revision		
BMC Revision		
SDR Revision		

NOTE: Bold text indicates default setting.

9.3.7 Event Logging Configuration Submenu

To access this submenu, select Advanced on the menu bar, then Event Logging Configuration.

Main	Advanced	Boot	Security	Exit
`CPU Configuration`				
`IDE Configuration`				
`Floppy Configuration`				
`SuperIO Configuration`				
`ACPI Configuration`				
`System Management Configuration`				
`Event Logging Configuration`				
`Fibre Channel Routing (PICMG)`				
`Remote Access Configuration`				
`USB Configuration`				
`PCI Configuration`				

Table 69 shows event logging configuration options.

Table 69. **Event Logging Configuration Submenu**

Feature	Options	Description
Event Logging	Disabled **Enabled**	Enable/Disable fatal error event logging.
ECC Memory Event Logging	Disabled **Enabled**	Enable/Disable MBE/SBE error logging.

Table 69. Event Logging Configuration Submenu

Non-Fatal Event Logging	Disabled **Enabled**	Enable/Disable Non-fatal error logging.
Assert NMI on Fatal Error	Disabled **Enabled**	Enable/Disable NMI assertion on fatal error events.
Clear Sel Event Log		Option to clear the event logs.

NOTE: Bold text indicates default setting.

9.3.8 Fibre Channel Routing (PICMG) Configuration Submenu

To access this submenu, select Advanced on the menu bar, then Fibre Channel Routing (PICMG) Configuration.

Main	Advanced	Boot	Security	Exit
CPU Configuration				
IDE Configuration				
Floppy Configuration				
SuperIO Configuration				
ACPI Configuration				
System Management Configuration				
Event Logging Configuration				
Fibre Channel Routing (PICMG)				
Remote Access Configuration				
USB Configuration				
PCI Configuration				

Table 70 shows how to configure Fibre Channel routing options.

Table 70. Fibre Channel Routing (PICMG) Submenu

Feature	Options	Description
Fibre Channel A	**Front** Back Disabled	Select Front/Back panel FC A connection.
Fibre Channel B	**Front** Back Disabled	Select Front/Back panel FC B connection.
Actual Fibre Channel Port A State	**NA**	Display actual Fibre Channel Port A routing.
Actual Fibre Channel Port B State	**NA**	Display actual Fibre Channel Port B routing.

NOTE: Bold text indicates default setting.

9.3.9 Remote Access Configuration Submenu

To access this submenu, select Advanced on the menu bar, then Remote Access Configuration.

Main	Advanced	Boot	Security	Exit
CPU Configuration				
IDE Configuration				
Floppy Configuration				
SuperIO Configuration				
ACPI Configuration				
System Management Configuration				
Event Logging Configuration				
Fibre Channel Routing (PICMG)				
Remote Access Configuration				
USB Configuration				
PCI Configuration				

Table 71 shows remote access configuration options.

Table 71. Remote Access Configuration Submenu

Feature	Options	Description
Remote Access	Disabled **Enabled**	Select remote access type.
Serial Port Number	**COM1**	Serial port for console redirection.
Serial Port Mode	115200 8, n, 157600 8, n, 119200 8, n, **9600 8, n, 1**	Serial port settings.
Flow Control	**None** Hardware Software	Select flow control for console redirection.
Redirection After BIOS POST	**Disabled** Boot Loader Always	Select the redirection method after the POST boot loader.
Terminal Type	**ANSI** VT 100 VT-UTF8	Select the target terminal type.
Send Carriage Return	**Disabled** Enabled	Enable this support if the target terminal has more than 80 columns.
VT-UTF8 Combo Key Support	**Disabled** Enabled	Enable VT-UTF8 Combination Key support for ANSI/VT100 terminals.

NOTE: **Bold** text indicates default setting.

9.3.10 USB Configuration Submenu

To access this submenu, select Advanced on the menu bar, then USB Configuration.

Main	Advanced	Boot	Security	Exit
`CPU Configuration`				
`IDE Configuration`				
`Floppy Configuration`				
`SuperIO Configuration`				
`ACPI Configuration`				
`System Management Configuration`				
`Event Logging Configuration`				
`Fibre Channel Routing (PICMG)`				
`Remote Access Configuration`				
`USB Configuration`				
`PCI Configuration`				

USB configuration options.

Table 72. USB Configuration Submenu

Feature	Options	Description
Legacy USB Support	Disabled **Enabled**	Enable legacy USB support.
USB Keyboard Legacy Support	Disabled **Enabled**	Enable legacy support of USB Keyboard.
USB Mouse Legacy Support	Disabled **Enabled**	Enable legacy support of USB Mouse.
USB Storage Device Legacy Support	Disabled **Enabled**	Enable legacy support of USB Mass Storage.
USB Mass Storage Reset Delay	10 sec **20 sec** 30 sec 40 sec	Number of seconds POST waits for USB mass storage device after unit command.
USB Beep Message	Disabled **Enabled**	Enable the beep during USB device enumeration.

NOTE: **Bold** text indicates default setting.

9.3.10.1 USB Mass Storage Device Configuration

Main	Advanced	Boot	Security	Exit
CPU Configuration				
IDE Configuration				
Floppy Configuration				
SuperIO Configuration				
ACPI Configuration				
System Management Configuration				
Event Logging Configuration				
Fibre Channel Routing (PICMG)				
Remote Access Configuration				
USB Configuration				
USB Mass Storage Device Configuration				

Table 73. USB Mass Storage Device Configuration

Feature	Options	Description
Device #		Display USB Mass Storage device(s) Name
Emulation Type	**Auto** Floppy Forced FDD Hard Disk CDROM	If Auto, USB devices less than 530 MByte are emulated as Floppy and remaining as hard drive. Forced FDD option can be used to force a HDD formatted drive to boot as FDD (Ex. ZIP drive).

9.3.11 PCI Configuration

To access this submenu, select Advanced on the menu bar, then USB Configuration.

Main	Advanced	Boot	Security	Exit
CPU Configuration				
IDE Configuration				
Floppy Configuration				
SuperIO Configuration				
ACPI Configuration				
System Management Configuration				
Event Logging Configuration				
Fibre Channel Routing (PICMG)				
Remote Access Configuration				
USB Configuration				
USB Mass Storage Device Configuration				
PCI Configuration				

The menu represented in the following table is used to configure USB options.

Table 74. PCI Configuration Submenu

Feature	Options	Description
Onboard Fibre Channel	Disabled **Enabled**	Enable/Disable Onboard Fibre Channels Option-ROM.
Onboard Gigabit LAN	Disabled **Enabled**	Enable/Disable Onboard Gigabit LAN Option-ROM

9.4 Boot Menu

To access this menu, select Boot from the menu bar at the top of the screen.

Main	Advanced	Boot	Security	Exit
`Boot Settings Configuration`				
`Boot Device Priority`				
`Hard Disk Drive Priority`				
`Removable Device Priority`				

The menu represented in the following table is used to set the boot features and the boot sequence.

Table 75. Boot Menu

Feature	Options	Description
Boot Settings Configuration	Select to display submenu	Set boot options
Boot Device Priority	Select to display submenu	Set first, second and last boot device.
Hard Disk Drive	Select to display submenu	Set first, second and last hard drive
OS Load Timeout Timer	Select to display submenu	Set first, second and last removable device

9.4.1 Boot Settings Configuration Submenu

To access this submenu, select Boot on the menu bar, then Boot Settings Configuration.

Main	Advanced	Boot	Security	Exit
`Boot Settings Configuration`				
`Boot Device Priority`				
`Hard Disk Drives`				
`OS Load Timeout Timer`				

The menu represented in the following table is used to configure Boot Settings.

Table 76. Boot Settings Configuration Submenu

Feature	Options	Description
Quick Boot	Disabled **Enabled**	Disable/Enable the BIOS to skip certain tests while booting, to decrease the time needed to boot the system.
Quiet Boot	**Disabled** Enabled	Display normal POST messaged/OEM logo.
AddOn ROM Display Mode	**Force BIOS** Keep Current	Set display mode for Option ROM
Bootup Num-Lock	Off **On**	Set power-on state for num-lock.
Typematic Rate	Slow **Fast**	Select keyboard Typematic Rate
System Keyboard	Absent **Present**	Enable/Disable all keyboards attached to the system.
Boot To OS/2	**No** Yes	OS/2 Compatibility mode.
Wait For ‘F1’ If Error	**Disabled** Enabled	Disable/enable waiting for F1 key to be pressed if error occurs.
Hit ‘DEL’ Message Display	Disabled **Enabled**	Display “Press DEL to run Setup” in POST.
Soft Reset	Disabled **Enabled**	Enable/Disable Soft Reset feature.
Interrupt 19 Capture	**Disabled** Enabled	Disable/enable the ability for option ROMs to trap interrupt 19.

NOTE: **Bold** text indicates default setting.

9.4.2 Boot Device Priority Submenu

To access this submenu, select Boot on the menu bar, then Boot Device Priority.

Main	Advanced	Boot	Security	Exit
Boot Settings Configuration				
Boot Device Priority				
Hard Disk Drives				
OS Load Timeout Timer				

The menu represented in the following table is used to configure boot device priority.

Table 77. Boot Device Priority Submenu

Feature	Options	Description
1st Boot Device	Hard Drive IBA 2 IBA 1	Set the first boot device.
2nd Boot Device	Same options as first boot device.	Set the second boot device.
Last Boot Device	Same options as first boot device.	Set the last boot device.

NOTE: A device only shows as an option if it is installed and detected by the BIOS during boot.

9.4.3 Hard Disk Drive Submenu

To access this submenu, select Boot on the menu bar, then Hard Disk Drive Priority.

Main	Advanced	Boot	Security	Exit
Boot Settings Configuration				
Boot Device Priority				
Hard Disk Drives				
OS Load Timeout Timer				

The menu represented in the following table is used to configure hard disk drive priority.

Table 78. Hard Disk Drive Priority Submenu

Feature	Options	Description
1st Hard Drive	IDE Hard Drive USB Hard Drive FC1 Hard Drive FC2 Hard Drive	Set the first hard drive.
2nd Hard Drive	Same options as first hard drive.	Set the second hard drive.

NOTE: A device only shows as an option if it is installed and detected by the BIOS during boot.

9.4.4 OS Load Timeout Timer

To access this submenu, select Boot on the menu bar, then OS Load Timeout Timer.

Main	Advanced	Boot	Security	Exit
Boot Settings Configuration				
Boot Device Priority				
Hard Disk Drives				
OS Load Timeout Timer				

Table 79. OS Load Timeout Timer Submenu

Feature	Options	Description
OS Load Timeout	**Disabled** 60sec 120 sec 150 sec 240 sec 480 sec 600 sec	Select the timeout value for OS load timer.
OS Load Action	Stay On **Reset** Power Off Power Cycle	Controls the action upon timeout.

9.5 Security Menu

To access this menu, select Security from the menu bar at the top of the screen.

Main	Advanced	Boot	Security	Exit

The menu represented by the following table is for setting passwords and security features.

Table 80. Security Menu

Feature	Options	Description
Supervisor Password		Display the Supervisor Password status. Installed/Not Installed
User Password		Display the Supervisor Password status. Installed/Not Installed
Change Supervisor Password		Set the supervisor password.
Change User Password		Set the user password.
Clear User Password		Clear the user password.
Boot Sector Virus Protection	**Disabled** Enabled	Disable/enable boot sector virus protection.

NOTE: Bold text indicates default setting.

9.6 Exit Menu

To access this menu, select Exit from the menu bar at the top of the screen.

Main	Advanced	Security	Boot	System Management	Exit

The menu represented in the following table is for exiting the BIOS Setup program, saving changes, and loading and saving defaults.

Table 81. Exit Menu

Feature	Options	Description
Save Changes and Exit		Exit system setup after saving changes.
Discard Changes and Exit		Exit system setup without saving changes.
Discard Changes		Discard changes without exiting.
Load Optimal Defaults		Load optimal default values.
Load FailSafe Defaults		Load failsafe default values.
Load Custom Defaults		Load custom default values.
Save Custom Defaults		Save custom default values.

Operating the Unit 10

10.1 BIOS Configuration

See Chapter 7, “BIOS Features,” for BIOS configuration options and Chapter 9, “BIOS Setup,” for information about using the BIOS Setup program. See Section 2.2.3.1, “Memory Ordering Rule for the MCH” on page 18 for information about installing DIMMs.

10.2 BIOS Image Updates

At times, new BIOS images will be released to add additional features to the SBC. The release package contains the flash utility, which comes in two versions. They are "flashdos" for DOS and "flashlnx" for Linux OS. The package also contains the BIOS ROM image. Below is a step-by-step procedure on how to update the BIOS:

1. Copy the flash utility and the Pxx-xxxx.rom file to a DOS bootable floppy disk.
2. Boot AT8000from a USB floppy disk (connected to the USB port) to a DOS prompt.
3. Copy flash utility and BIOS ROM image to RAM disk, which is automatically generated (C: drive).
4. Issue the command "flashdos /b Pxx-xxxx (xx= build type version, xxxx=build identifier).
5. Enter "Y" to overwrite the BIOS on the board.
6. Enter "Y" to clear the current COMS settings on the board.
7. Enter "Y" to reboot the system after the BIOS has been upgraded successfully.

10.3 Procedures to Copy and Save CMOS Settings

The CMOS settings can be copied to a file with a file name specified by the user and saved into a directory.

10.3.1 Copying CMOS.bin from the SBC

1. Copy the flashlnx utility to the SBC running MontaVista Carrier Grade Linux.
2. Issue the command "./flashlnx -bc CMOS.bin" to copy the CMOS settings to the same directory from which flashlnx is executed.

All user preferred settings are saved on the file named CMOS.bin.

10.3.2 Saving CMOS.bin to the SBC

1. Copy the flashlnx utility and CMOS.bin to the SBC running MontaVista Carrier Grade Linux.
2. Execute "chmod +x flashlnx" to change the file attribute to executable form.
3. Execute "./flashlnx -rc CMOS.bin" to copy the CMOS.bin file to the CMOS.
4. Upon completion, perform a reset to ensure the new CMOS settings are loaded.

10.3.3 Error Messages

The table below lists and defines the possible error messages that may occur.

Table 82. Error Messages

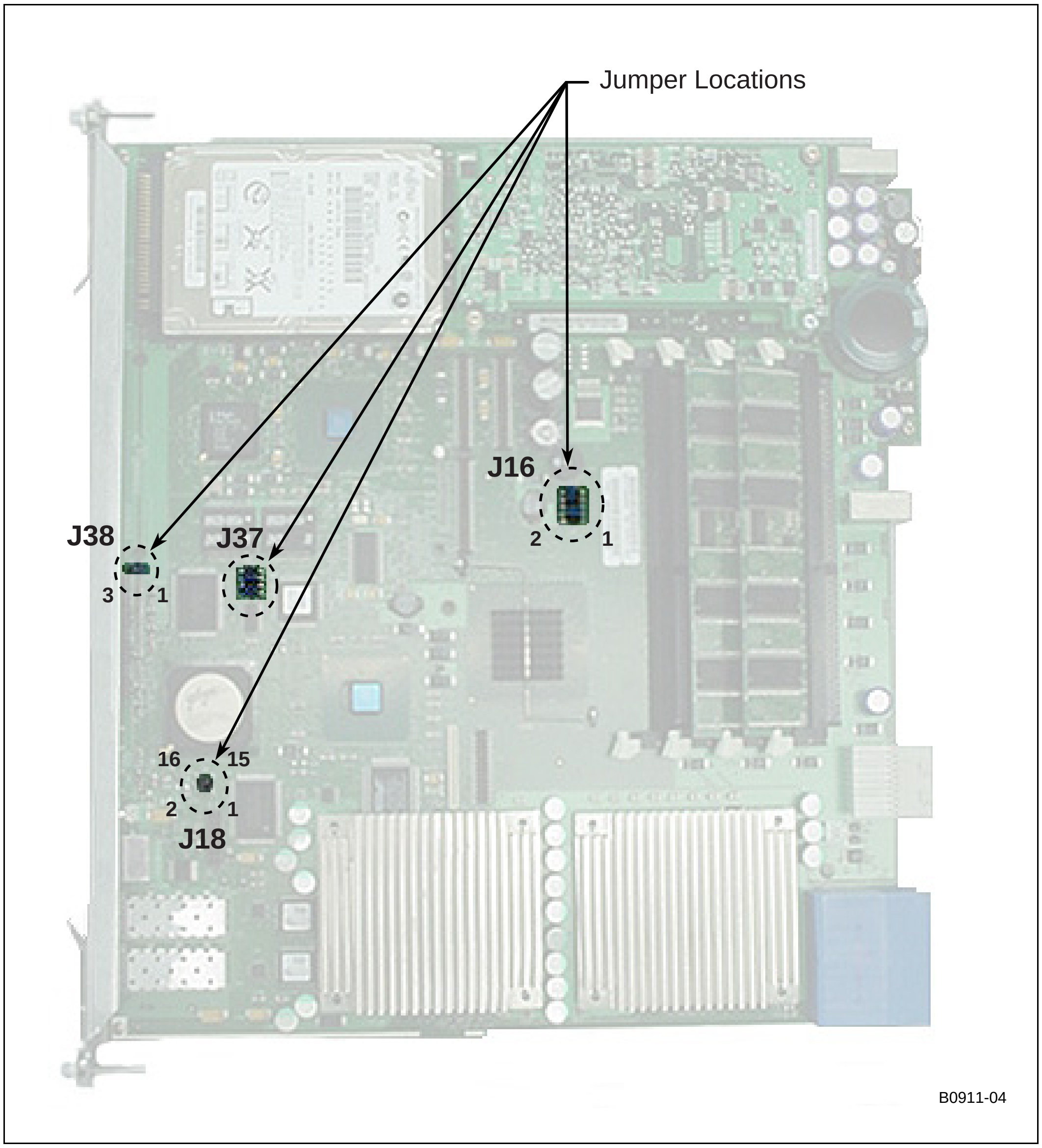
Message	Definition	Notes
CMOS Buffer has bad checksum	CMOS file is corrupted	The utility will not allow the user to update the CMOS settings.
CMOS backup/restore is not supported	CMOS restore operation is not possible.	This happens if the user attempts to restore CMOS settings on non-SBC boards.
Data ID not found	CMOS area is not detected in BIOS.	Only applies to boards having this feature.
You are updating the CMOS with settings not for this BIOS. It may cause your system to be unable to boot next time.	The CMOS file is not valid for the current BIOS.	The user should abort the operation.

10.4 Jumpers

The AT8000 contains several jumper posts that allow the user to configure certain options not configurable through the BIOS Setup Utility. The “Jumper Locations” figure below shows the placement of the AT8000 jumpers. See Table 84, “Jumper Definitions” on page 122 for the function of each jumper.

Note: The AT8000 is shipped pre-configured—jumper positions do not need to be altered.

Figure 24. Jumper/Connector Locations



Note: Pin 2 is directly beside pin 1 and is marked on the board silkscreen. The back row has odd-numbered pins and the front row has even-numbered pins.

Table 83. J18 Pin Assignments

Lattice* Compatible JTAG Header	PS/2 Keyboard/Mouse Header
1 +3.3 VSB	2 MDAT (PS/2 mouse data)
3 TDO	4 MCLK (PS/2 mouse clock)
5 TDI (H0_SKTOCC#)	6 GND
7 ISPEN#	8 +5 V (through polyswitch)
9 Key - no pin or connection	10 KBDAT (PS/2 keyboard data)
11 TMS (H1_SKTOCC#)	12 KBCLK (PS/2 keyboard clock)
13 GND	14 Key - no pin or connection
15 TCK (WDT_EN)	16 GND

NOTE: Processors must be removed before using the Lattice JTAG interface.

Table 84. Jumper Definitions

Jumper	Function
J16-1 to 3	CLEAR_PASSWD: This jumper is used in the event the system will not boot because the BIOS password is unknown.
J16-3 to 5	CLEAR_CMOS: This jumper is used in the unlikely event a CMOS data corruption keeps the system from booting (or getting to SETUP).
J16-4 to 6	RTC_RST: Hardware Reset of RTC. When asserted, this signal resets register bits in the RTC well and sets the RTC_PWR_STS bit (bit 2 in GEN_PMCON3 register).
J16-2 to 4	FRC_UPD (IPMC F/W): This jumper is used to put the firmware into a forced update mode. Administrators could use this feature to force the firmware to enter into update mode and wait for an update through the KCS interface. Useful when some of the SDR or firmware needs to change. Please note that Sensor scanning/ monitoring is disabled in this mode. Administrators will have to remember to disable the jumper after an update, or the board will boot again into this update mode.
J16-3 to 4 and J16-7 to 9 (Default)	Storage posts for jumpers not in use.
J16-8 to 7	Only for debug purposes.
J16-10 to 9	Manufacturing jumper (for testing during board assembly).

10.5 Digital Ground to Chassis Ground Connectivity

In the default grounding for MPCBL0001xxx, digital ground is isolated from the chassis ground.

Table 85. Ground Jumper (J38)

Jumper	Digital to Chassis Ground Planes
J38-1 to 2	Isolated
J38-2 to 3	Connected

Note: Digital Ground is also called Logic Ground. Chassis Ground is also called Shelf Ground.

To connect the digital ground to the chassis ground, remove the jumper connecting J38-1 to 2 and place it on jumper position 2-3.

Maintenance 11

11.1 Supervision

There are four main components that perform hardware monitoring of voltages and timers. They are listed in the table below.

Table 86. Hardware Monitoring Components

Component	Function	Monitors
Intelligent Platform Management Controller	WDT #1	Commands from the BIOS. If the timer expires (times out), causes a soft or hard reset.
Heceta-5 (ADM1026)	Analog-to-Digital converter	Voltages: +1.2 V, +1.5 V, +1.8 V, +3.3 VSB, +5 VSB, VCPU, VTTDDR, +2.5 V, +12 V, -12 V, +5 V, SuperCap (VBAT), IPMB_V, +1.8 VSB.
ICH3 (82801CA I/O Controller Hub 3)	WDT #3	The first attempt to fetch an instruction after a power failure.
PLD (2064VE)	WDT #2	Strobes by IPMC firmware. If it expires, it isolates AT8000 from the backplane IPMB buses and resets the IPMC.

11.2 Diagnostics

11.2.1 In-Target Probe (ITP)

The ITP connector allows connection of a tool that helps you observe and control the step-by-step execution of your program for debugging hardware and software. Debugging includes finding a hardware or software error and identifying the location and cause of the error so it can be corrected.

Intel continually looks for ways to maximize the development and delivery of mission critical tools to our internal validation teams and strategic OEM customers. As a result, Intel has put together a third-party vendor program team. This team works with third-party vendors to develop and deliver specific tools formerly supplied by Intel to internal and external customers.

Intel recommends visiting any of the Website URLs below, and selecting a vendor of your choice to provide in-circuit emulation hardware and software.

- American Arium* currently develops in-circuit emulation and run control tools for Intel processors for use by Intel BIOS and driver teams, Intel manufacturing, and OEM customers.

http://www.arium.com/

- Agilent Technologies* currently develops logic analyzer and probing tools for Intel processors for use by Intel validation teams (chip, system, platform) and OEM customers.

http://we.home.agilent.com

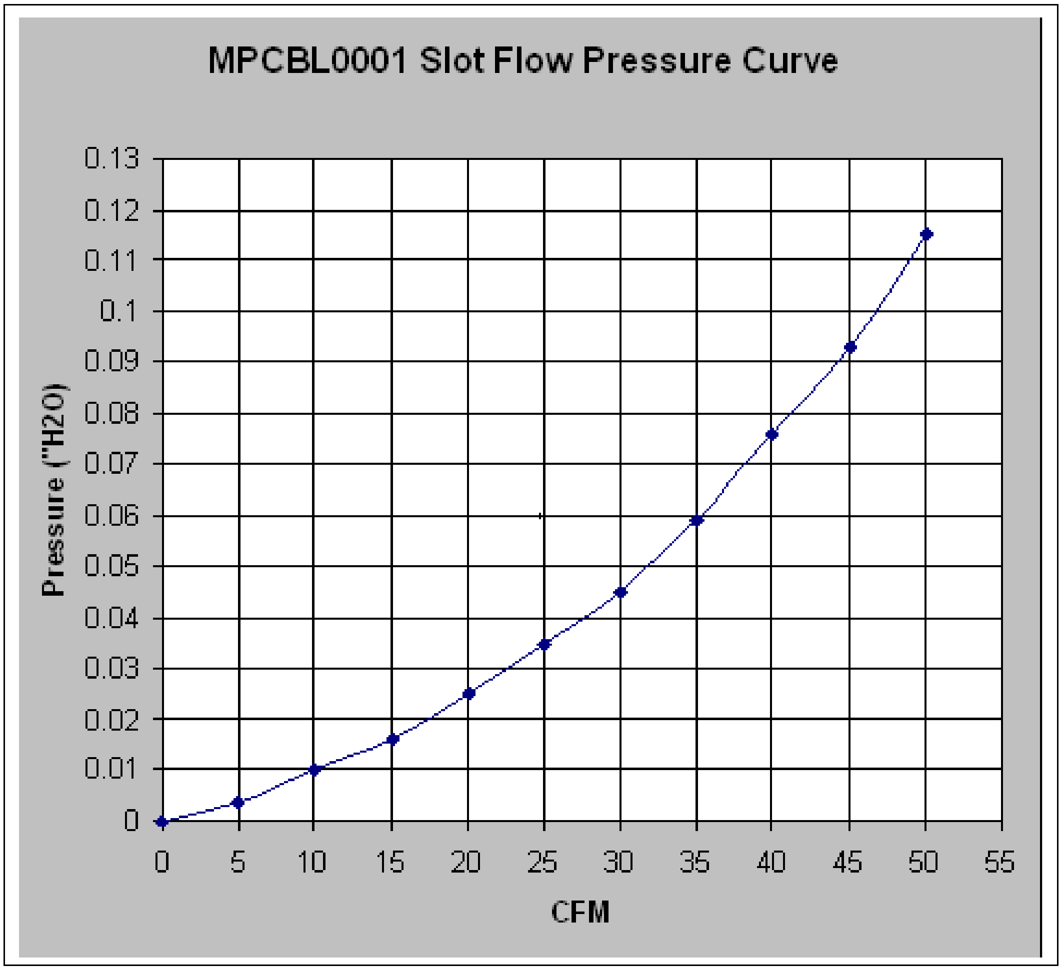
- Tektronix* currently develops logic analyzer and probing tools for Intel processors for use by Intel validation teams (chip, system, platform) and OEM customers.

http://www.tek.com/Measurement/logic_analyzers/index.html

Thermals 12

The pressure drop curves versus the flow rate in Figure 25 represents flow impedance of the slot This information is provided in accordance with Section 5 of the PICMG 3.0 Specification. It will aid the system integrator in using the AT8000 SBC in various AdvancedTCA* shelves.

Figure 25. Power vs. Flow Rate



Component Technology 13

The main components implemented on the Kontron AT8000 are listed in the table below.

Table 87. Main Components

Code Name	Brand Name	Package Type
LP Prestonia	Low Voltage Intel® Xeon™ processor	FCPGA2, Socket 604
ICH3	Intel® 82801CA I/O Controller Hub 3	421-ball, BGA
P64H2	Intel® 82870P2 64-bit PCI/PCI-X Controller Hub 2	567-ball, FC-BGA
Plumas 533	Intel® E7501 chipset	N/A
Plumas MCH	Intel® E7501 Memory Controller Hub	1005-ball, FC-BGA
Anvik	Intel® 82546 Dual Gigabit Ethernet Controller	364 -ball, TFBGA
Super I/O	Standard Microsystems Corp.* LPC47B272	100-pin, QFP
Fibre Channel Controller	Qlogic Corp.* ISP2312	388-ball, EPBGA-T
Fibre Channel Controller SRAM	Micron Semiconductor* MT58L256L118F	165-ball, FBGA
IPMC	Intel® IPMC	156-ball, BGA
FWH	Intel® 82802AC Firmware Hub	32-pin, PLCC.

Warranty Information 14

14.1 Limited Warranty

Kontron Canada, Inc, ("The seller") warrants its boards to be free from defects in material and workmanship for a period of two (2) years commencing on the date of shipment. The liability of the seller shall be limited to replacing or repairing, at the seller's option, any defective units. Equipment or parts, which have been subject to abuse, misuse, accident, alteration, neglect, or unauthorized repair are not covered by this warranty. This warranty is in lieu of all other warranties expressed or implied.

14.2 Returning a Defective Product (RMA)

At Kontron, we take great pride in our customers' successes. We believe in providing full support at all stages of your product development.

If at any time you encounter difficulties with your application or with any of our products, or if you simply need guidance on system setups and capabilities, contact our Technical Support at:

CANADIAN HEADQUARTERS

Tel. (450) 437-5682

Fax: (450) 437-8053

If you have any questions about Kontron, our products, or services, visit our Web site at: www.kontron.com

You also can contact us by E-mail at: support@ca.kontron.com

Or at the following address:

Kontron Canada, Inc.

616 Curé Boivin

Boisbriand, Québec

J7G 2A7 Canada

RETURNING DEFECTIVE MERCHANDISE

Before returning any merchandise please do one of the following if your product malfunctions:

Call

1. Call our Technical Support department in Canada at (450) 437-5682. Make sure you have the following on hand: our Invoice #, your Purchase Order #, and the Serial Number of the defective unit.

2. Provide the serial number found on the back of the unit and explain the nature of your problem to a service technician.

3. The technician will instruct you on the return procedure if the problem cannot be solved over the telephone.

4. Make sure you receive an RMA # from our Technical Support before returning any merchandise.

Fax

1. Make a copy of the request form on the following page.

2. Fill it out.

3. Fax it to us at: (450) 437-8053

E-mail

1. Send us an e-mail at: RMA@ca.kontron.com. In the e-mail, you must include your name, your company name, your address, your city, your postal/zip code, your phone number, and your e-mail. You must also include the serial number of the defective product and a description of the problem.

When returning a unit.

i) In the box, you have to include the name and telephone number of a person whom we can contact for further explanations if necessary when returning goods. Where applicable, always include all duty papers and invoice(s) associated with the item(s) in question.

ii) Ensure that the unit is properly packed. Pack it in a rigid cardboard box.

iii) Clearly write or mark the RMA number on the outside of the package you are returning.

iv) Ship prepaid. We take care of insuring incoming units.

Kontron Canada Inc.

616 Curé Boivin

Boisbriand, Québec

J7G 2A7 Canada

Contact Name: ______________________________

Company Name: ______________________________

Street Address: ______________________________

City:	____________	Province/State:	____________
Country:	____________	Postal/Zip Code:	____________
Phone Number:	____________	Extension:	____________
Fax Number:	____________	E-Mail:	____________

Serial Number	Failure or Problem Description	P.O. # (if not under warranty)

Kontron Canada, Inc., 616 Curé Boivin, Boisbriand, Québec, Canada, J7G 2A7

Fax this form to Kontron's Technical Support department in Canada at (450) 437-8053

Certifications 15

The Intel® NetStructure™ MPCBL0001 High-Performance Single Board Computer has the following approvals:

- UL/cUL 60950
- EN/IEC 60950
- EN55022 Class A
- EN55024
- FCC CFR47 Part 15 Class A
- VCCI
- AS/NZS3548
- BSMI

Agency Information 16

16.1 North America (FCC Class A)

FCC Verification Notice

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For questions related to the EMC performance of this product, contact:

Intel Corporation
5200 N.E. Elam Young Parkway
Hillsboro, OR 97124
1-800-628-8686

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the use will be required to correct the interference at his own expense.

16.2 Canada – Industry Canada (ICES-003 Class A) (English and French-translated)

CANADA – INDUSTRY CANADA

Cet appareil numérique respecte les limites bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: “Appareils Numériques”, NMB-003 édictée par le Ministre Canadian des Communications.

(English translation of the notice above) This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the interference-causing equipment standard entitled “Digital Apparatus,” ICES-003 of the Canadian Department of Communications.

16.3 Safety Instructions (English and French-translated)

16.3.1 English

CAUTION: This equipment is designed to permit the connection of the earthed conductor of the d.c. supply circuit to the earthing conductor at the equipment. See installation instructions. If this connection is made, all of the following conditions must be met:

-This equipment shall be connected directly to the DC supply system earthing electrode conductor or to a bonding jumper from an earthing terminal bar or bus to which the DC supply system earthing electrode conductor is connected.

-This equipment shall be located in the same immediate area (such as adjacent cabinets) as any other equipment that has a connection between the earthed conductor of the same DC supply circuit and the earthing conductor, and also the point of earthing of the DC system. The DC system shall not be earthed elsewhere.

-The DC supply source shall be located within the same premises as this equipment.

-Switching or disconnecting devices shall to be in the earthed circuit conductor between the DC source and the point of connection of the earthing electrode conductor.

16.3.2 French

Cet appareil est conçu pour permettre le raccordement du conducteur relié à la terre du circuit d'alimentation c.c. au conducteur de terre de l'appareil. Cet appareil est conçu pour permettre le raccordement du conducteur relié à la terre du circuit d'alimentation c.c. au conducteur de terre de l'appareil. Pour ce raccordement, toutes les conditions suivantes doivent être respectées:

- Ce matériel doit être raccordé directement au conducteur de la prise de terre du circuit d'alimentation c.c. ou à une tresse de mise à la masse reliée à une barre omnibus de terre laquelle est raccordée à l'électrode de terre du circuit d'alimentation c.c.

- Les appareils dont les conducteurs de terre respectifs sont raccordés au conducteur de terre du même circuit d'alimentation c.c. doivent être installés à proximité les uns des autres (p.ex., dans des armoires adjacentes) et à proximité de la prise de terre du circuit d'alimentation c.c. Le circuit d'alimentation c.c. ne doit comporter aucune autre prise de terre. matériel. - Il ne doit y avoir

– La source d'alimentation du circuit c.c. doit être située dans la même pièce que le aucun dispositif de commutation ou de sectionnement entre le point de raccordement au conducteur de la source d'alimentation c.c. et le point de raccordement à la prise de terre.

Safety Warnings 17

Caution: Review the following precautions to avoid personal injury and prevent damage to this product or products to which it is connected. To avoid potential hazards, use the product only as specified.

Read all safety information provided in the component product user manuals and understand the precautions associated with safety symbols, written warnings, and cautions before accessing parts or locations within the unit. Save this document for future reference.

AC AND/OR DC POWER SAFETY WARNING: The AC and/or DC Power cord is the unit's main AC and/or DC disconnecting device, and must be easily accessible at all times. Auxiliary AC and/or DC On/Off switches and/or circuit breaker switches are for power control functions only (NOT THE MAIN DISCONNECT).

IMPORTANT: See installation instructions before connecting to the supply.

For AC systems, use only a power cord with a grounded plug and always make connections to a grounded main. Each power cord must be connected to a dedicated branch circuit.

For DC systems, this unit relies on the building's installation for short circuit (over-current) protection. Ensure that a Listed and Certified fuse or circuit breaker no larger than 72VDC, 15A is used on all current carrying conductors. For permanently connected equipment, a readily accessible disconnect shall be incorporated in the building installation wiring. For permanent connections, use copper wire of the gauge specified in the system's user manual.

The enclosure provides a separate Earth ground connection stud. Make the Earth ground connection prior to applying power or peripheral connections and never disconnect the Earth ground while power or peripheral connections exist.

To reduce the risk of electric shock from a telephone or Ethernet* system, connect the unit's main power before making these connections. Disconnect these connections before removing main power from the unit.

RACK MOUNT ENCLOSURE SAFETY: This unit may be intended for stationary rack mounting. Mount in a rack designed to meet the physical strength requirements of NEBS GR-63-CORE and NEBS GR 487. Disconnect all power sources and external connections prior to installing or removing the unit from a rack.

System weight may be minimized prior to mounting by removing all hot-swappable equipment. Mount your system in a way that ensures even loading of the rack. Uneven weight distribution can result in a hazardous condition. Secure all mounting bolts when rack mounting the enclosure.

Warning: Verify power cord and outlet compatibility: Use the appropriate power cords for your power outlet configurations. Visit the following website for additional information: http://kropla.com/electric2.htm.

Warning: Avoid electric overload, heat, shock, or fire hazard: Only connect the system to a to a properly rated supply circuit as specified in the product user manual. Do not make connections to terminals outside the range specified for that terminal. See the product user manual for correct connections.

Warning: Avoid electric shock: Do not operate in wet, damp, or condensing conditions. To avoid electric shock or fire hazard, do not operate this product with enclosure covers or panels removed.

Warning: Avoid electric shock: For units with multiple power sources, disconnect all external power connections before servicing.

Warning: Power supplies must be replaced by qualified service personnel only.

Caution: System environmental requirements: Components such as Processor Boards, Ethernet Switches, etc., are designed to operate with external airflow. Components can be destroyed if they are operated without external airflow. External airflow is normally provided by chassis fans when components are installed in compatible chassis. Never restrict the airflow through the unit's fan or vents. Filler panels or air management boards must be installed in unused chassis slots. Environmental specifications for specific products may differ. Refer to product user manuals for airflow requirements and other environmental specifications.

Warning: Device heatsinks may be hot during normal operation: To avoid burns, do not allow anything to touch heatsinks.

Warning: Avoid injury, fire hazard, or explosion: Do not operate this product in an explosive atmosphere.

Caution: Lithium batteries. There is a danger of explosion if a battery is incorrectly replaced or handled. Do not disassemble or recharge the battery. Do not dispose of the battery in fire. When the battery is replaced, the same type (CR2032) or an equivalent type recommended by the manufacturer must be used. Used batteries must be disposed of according to the manufacturer's instructions.

Warning: Avoid injury: This product may contain one or more laser devices that are visually accessible depending on the plug-in modules installed. Products equipped with a laser device must comply with International Electrotechnical Commission (IEC) 60825.

17.1 Mesures de sécurité

Veuillez suivre les mesures de sécurité suivantes pour éviter tout accident corporel et ne pas endommager ce produit ou tout autre produit lui étant connecté. Pour éviter tout danger, veillez à utiliser le produit conformément aux spécifications mentionnées.

Lisez toutes les informations de sécurité fournies dans les manuels de l'utilisateur des produits composants et veillez à bien comprendre les mesures associées aux symboles de sécurité, aux avertissements écrits et aux mises en garde avant d'accéder à certains éléments ou emplacements de l'unité. Conservez ce document comme outil de référence.

AVERTISSEMENT CONCERNANT LA SÉCURITÉ DE L'ALIMENTATION C.A. ET/OU C.C. : le câble d'alimentation C.A. et/ou C.C. constitue le dispositif de déconnexion principal de l'alimentation électrique de l'unité et doit être facilement accessible à tous moments. Les commutateurs de marche/arrêt C.A. et/ou C.C. et/ou les commutateurs disjoncteurs auxiliaires permettent uniquement de contrôler l'alimentation (ET NON LA DÉCONNEXION PRINCIPALE).

IMPORTANT : reportez-vous aux instructions d'installation avant de connecter le bloc d'alimentation.

Pour les systèmes C.A., utilisez uniquement un câble d'alimentation avec une prise de terre et établissez toujours les connexions à une prise secteur mise à la terre. Chaque câble d'alimentation doit être connecté à un circuit terminal dédié.

Pour les systèmes C.C., la protection de cette unité repose sur les coupe-circuits (surintensité) du bâtiment. Assurez-vous d'utiliser un fusible ou un disjoncteur répertorié et certifié ne dépassant pas 72 VCC et 15 A pour tous les conducteurs de courant. Pour les équipements connectés en permanence, un sectionneur facilement accessible doit être incorporé au câblage du bâtiment. Pour les connexions permanentes, utilisez des câbles en cuivre d'un calibre conforme à celui spécifié dans le manuel de l'utilisateur du système.

Le boîtier fournit un connecteur de mise à la terre séparé. Établissez la connexion à la terre avant de mettre le système sous tension ou de connecter des périphériques. Veillez à ne jamais déconnecter la mise à la terre tant que le système est sous tension ou si des périphériques sont connectés.

Pour réduire le risque d'un choc électrique en provenance d'un téléphone ou d'un système Ethernet*, connectez l'alimentation principale de l'unité avant d'établir ces connexions. De même, déconnectez-les avant de couper l'alimentation principale de l'unité.

SÉCURITÉ DU BOÎTIER POUR UN MONTAGE EN BAIE : cette unité peut être destinée à un montage en baie stationnaire. Le montage en baie doit satisfaire aux exigences sur la résistance physique des normes NEBS GR-63-CORE et NEBS GR 487. Déconnectez toutes les sources d'alimentation et les connexions externes avant d'installer ou de supprimer l'unité d'une baie.

Minimisez la masse du système avant le montage en retirant l'équipement permutable à chaud. Assurez-vous que le système est réparti de manière uniforme sur la baie. Une distribution inégale de la masse du système peut présenter des risques. Fixez tous les boulons lors de l'installation du boîtier dans une baie.

Avertissement : vérifiez que le câble d'alimentation et la prise sont compatibles. Utilisez les câbles d'alimentation correspondant à la configuration de vos prises de courant. Pour de plus amples informations, visitez le site Web suivant : http://kropla.com/electric2.htm.

Avertissement : évitez toute forme de surcharge, chaleur, choc électrique ou incendie. Connectez uniquement le système à un circuit d'alimentation dûment répertorié conformément aux spécifications du manuel de l'utilisateur du produit. N'établissez pas de connexions à des terminaux en dehors des limites spécifiées pour ce terminal. Reportez-vous au manuel de l'utilisateur du produit pour les connections adéquates.

Avertissement : évitez les chocs électriques. N'utilisez pas ce produit dans des endroits humides, mouillés ou provoquant de la condensation. Pour éviter tout risque de choc électrique ou d'incendie, n'utilisez pas ce produit si les couvercles ou les panneaux du boîtier ne sont pas en place.

Avertissement : évitez les chocs électriques. Pour les unités comportant plusieurs sources d'alimentation, déconnectez toutes les sources d'alimentation externes avant de procéder aux réparations.

Avertissement : les blocs d'alimentation doivent être remplacés exclusivement par des techniciens d'entretien qualifiés.

Attention : exigences environnementales du système : les composants tels que les cartes de processeurs, les commutateurs Ethernet, etc., sont conçus pour fonctionner avec un flux d'air externe. Les composants peuvent être détruits s'ils fonctionnent dans d'autres conditions. Le flux d'air externe est généralement produit par les ventilateurs des châssis lorsque les composants sont installés dans des châssis compatibles. Veillez à ne jamais obstruer le flux d'air alimentant le ventilateur ou les conduits de l'unité. Des boucliers ou des panneaux de gestion de l'air doivent être installés dans les connecteurs inutilisés du châssis. Les spécifications environnementales peuvent varier d'un produit à un autre. Veuillez-vous reporter au manuel de l'utilisateur pour déterminer les exigences en matière de flux d'air et d'autres spécifications environnementales.

Avertissement : les dissipateurs de chaleur de l'appareil peuvent être chauds lors d'un fonctionnement normal. Pour éviter tout risque de brûlure, veillez à ce que rien n'entre en contact avec les dissipateurs de chaleur.

Avertissement : évitez les blessures, les incendies ou les explosions. N'utilisez pas ce produit dans une atmosphère présentant des risques d'explosion.

Attention : les batteries au lithium. Celles-ci peuvent exploser si elles sont incorrectement remplacées ou manipulées. Veillez à ne pas désassembler ni à recharger la batterie. Veillez à ne pas jeter la batterie au feu. Lors du remplacement de la batterie, utilisez le même type de batterie (CR2032) ou un type équivalent recommandé par le fabricant. Les batteries usagées doivent être mises au rebut conformément aux instructions du fabricant.

Avertissement : évitez les blessures. Ce produit peut contenir un ou plusieurs périphériques laser visuellement accessibles en fonction des modules plug-in installés. Les produits équipés d'un périphérique laser doivent être conformes à la norme IEC (International Electrotechnical Commission) 60825.

Reference Documents A

The following documents should be available when using this specification. Documents that are not available on websites may be obtained from your IBL (Intel Business Link) account, or contact your Intel Field Sales Engineer (FSE) or Field Application Engineer (FAE).

- Qlogic* ISP2312 Intelligent Fibre Channel Processor data Sheet, 83312-508-00 B, March 19, 2002 (http://www.qlogic.com/products/isp_series/isp2300.asp)
- Standard Microsystems Corporation*, SMSC LPC47B27x Datasheet, Rev. 6/21/99 (http://www.smsc.com/main/catalog/lpc47b27x.html)
- Draft Standard Physical and Environmental Layers for PCI Mezzanine Cards: PMC IEEE* (MMSC) P1386.1/Draft 2.3, October 9, 2000
- Draft Standard for a Common Mezzanine Card Family: CMC. IEEE (MMSC) P1386/Draft 2.3, October 9, 2000
- AdvancedTCA Specification (http://www.advancedtca.org)

The following Intel Corporation documents may be required for more detailed information:

- Intel® NetStructure™ MPCHC0001 14U Shelf Technical Product Specification (http://www.intel.com/design/network/products/cbp/atca/MPCHC0001.htm)
- Intel® NetStructure™ MPCMM0001 Chassis Management Module Hardware Technical Product Specification (http://www.intel.com/design/network/products/cbp/atca/mpcmm0001.htm)
- Intel® NetStructure™ MPCMM0001 Chassis Management Module Software Technical Product Specification (http://www.intel.com/design/network/products/cbp/atca/mpcmm0001.htm)
- Low Voltage Intel® Xeon™ processor Product Page(http://www.intel.com/products/server/processors/server/xeon/index.htm?iid=ipp_srvr_proc+xeon512kb&)
- Intel® E7501 Chipset Datasheet: Intel E7501 Memory Controller Hub (MCH) (http://www.intel.com/design/chipsets/e7501/)
- Intel® 82801CA I/O Controller Hub 3 (ICH3-S) Datasheet (http://www.intel.com/design/chipsets/datashts/index.htm)
  plus the specification update (http://www.intel.com/design/chipsets/e7500/specupdt/)
- Intel® 82546 Gigabit Ethernet Controllers with Integrated PHY Network Silicon Product Brief (http://www.intel.com/design/network/prodbrf/82546EB_prodbrief.htm)
- 82546 Gigabit Ethernet Controllers with Integrated PHY Product Page (http://www.intel.com/design/network/products/lan/controllers/82546.htm)
- ITP700 Debug Port Design Guide (http://www.intel.com/design/Xeon/guides/)
- Low Voltage Intel® Xeon™ Processor Datasheet (http://www.intel.com/design/intarch/datashts/273766.htm)
- Intelligent Platform Management Interface v1.5 Specification (http://developer.intel.com/design/servers/ipmi/spec.htm)
- Intelligent Platform Management Interface Implementer's Guide (http://developer.intel.com/design/servers/ipmi/spec.htm)

- Low Pin Count (LPC) Interface Specification (http://developer.intel.com/design/chipsets/industry/lpc.htm)
- Intel® Boot Agent. (http://www.intel.com/support/network/adapter/pro100/bootagent/manual.htm)
- Intel's AdvancedTCA product line http://developer.intel.com/technology/atca/

List of Supported Commands (IPMI v1.5 and PICMG 3.0) B

Table 88. IPMI 1.5 Supported Commands (Sheet 1 of 3)

IPM Device Global Commands			
Command	**NetFn***	**CMD**	**IPMI 1.5 Spec Func**
Get Device ID	App	01h	17.1
Cold Reset	App	02h	17.2
Get Self Test Results	App	04h	17.4
Broadcast "Get Device ID"	App	?	17.9
BMC Watchdog Timer Commands			
Command	**NetFn***	**CMD**	**IPMI 1.5 Spec Func**
Reset Watchdog Timer	App	22h	21.5
Set Watchdog Timer	App	24h	21.6
Get Watchdog Timer	App	25h	21.7
BMC Device and Messaging Commands			
Command	**NetFn***	**CMD**	**IPMI 1.5 Spec Func**
Set IPMC Global Enables	App	2Eh	18.1
Get IPMC Global Enables	App	2Fh	18.2
Clear Message Flags	App	30h	18.3
Get Message Flags	App	31h	18.4
Get Message Flags	App	33h	18.6
Send Message	App	34h	18.7
Read Event Message Buffer	App	35h	18.8
Master Write-Read	App	52h	18.10
Set Channel Access	App	40h	18.20
Get Channel Access	App	41h	18.21
Get Channel Info	App	42h	18.22
Chassis Device Commands			
Command	**NetFn***	**CMD**	**IPMI 1.5 Spec Func**
Get Chassis Capabilities	Chassis	00h	22.1
Chassis Identity	Chassis	04h	22.5
Get POH Counter	Chassis	0Fh	22.12

Table 88. IPMI 1.5 Supported Commands (Sheet 2 of 3)

Event Commands			
Command	**NetFn***	**CMD**	**IPMI 1.5 Spec Func**
Set Event Receiver	S/E	00h	23.1
Get Event Receiver	S/E	01h	23.2
Platform Event (Event Message)	S/E	02h	23.3
PEF and Alerting Commands			
Command	**NetFn***	**CMD**	**IPMI 1.5 Spec Func**
Get PEF Capabilities	S/E	10h	24.1
Arm PEF Postpone Timer	S/E	11h	24.2
Set PEF Configuration Parameters	S/E	12h	24.3
Get PEF Configuration Parameters	S/E	13h	24.4
Set Last Processed Event ID	S/E	14h	24.5
Get Last Processed Event ID	S/E	15h	24.6
Alert Immediate	S/E	16h	24.7
PET Acknowledge	S/E	17h	24.8
Sensor Device Commands			
Command	**NetFn***	**CMD**	**IPMI 1.5 Spec Func**
Get Device SDR Info	S/E	20h	29.2
Get Device SDR	S/E	21h	29.3
Reserve Device SDR Repository	S/E	22h	29.4
Set Sensor Hysteresis	S/E	24h	29.6
Get Sensor Hysteresis	S/E	25h	29.7
Set Sensor Threshold	S/E	26h	29.8
Get Sensor Threshold	S/E	27h	29.9
Set Sensor Event Enable	S/E	28h	29.10
Get Sensor Event Enable	S/E	29h	29.11
Re-arm Sensor Events	S/E	2Ah	29.12
Get Sensor Event Status	S/E	2Bh	29.13
Get Sensor Reading	S/E	2Dh	29.14
FRU Device Commands			
Command	**NetFn***	**CMD**	**IPMI 1.5 Spec Func**
Get FRU Inventory Area Info	Storage	10h	28.1
Read FRU Data	Storage	11h	28.2
Write FRU Data	Storage	12h	28.3

Table 88. IPMI 1.5 Supported Commands (Sheet 3 of 3)

SDR Device Commands			
Command	**NetFn***	**CMD**	**IPMI 1.5 Spec Func**
Run Initialization Agent	Storage	2Ch	27.21
SEL Device Commands			
Command	**NetFn***	**CMD**	**IPMI 1.5 Spec Func**
Get SEL Info	Storage	40h	25.2
Get SEL Allocation Info	Storage	41h	25.3
Reserve SEL	Storage	42h	25.4
Get SEL Entry	Storage	43h	25.5
Add SEL Entry	Storage	44h	25.6
Partial Add SEL Entry	Storage	45h	25.7
Delete SEL Entry	Storage	46h	25.8
Clear SEL	Storage	47h	25.9
Get SEL Time	Storage	48h	25.10
Set SEL Time	Storage	49h	25.11
NOTE: *Refer to IPMI 1.5 Specifications for a detailed explanation on NetFn.			

Table 89. PICMG 3.0 IPMI Supported Commands

Command	Net Function	Command	Interface
Get PICMG Properties	2Ch	00h	SMS/SMM/IPMB
Get Address Info	2Ch	01h	SMS/SMM/IPMB
FRU Control	2Ch	04h	SMS/SMM/IPMB
Get FRU LED Properties	2Ch	05h	SMS/SMM/IPMB
Get LED Color Properties	2Ch	06h	SMS/SMM/IPMB
Set FRU LED State	2Ch	07h	SMS/SMM/IPMB
Get FRU LED State	2Ch	08h	SMS/SMM/IPMB
Set IPMB State	2Ch	09h	SMS/SMM/IPMB
Set FRU Activation Policy	2Ch	0Ah	IPMB
Get FRU Activation Policy	2Ch	0Bh	SMS/SMM/IPMB
Set FRU Activation	2Ch	0Ch	SMS/SMM/IPMB
Get Device Locator Record ID	2Ch	0Dh	SMS/SMM/IPMB
Set Port State	2Ch	0Eh	IPMB
Get Port State	2Ch	0Fh	SMS/SMM/IPMB
Compute Power Properties	2Ch	10h	SMS/SMM/IPMB
Set Power Level	2Ch	11h	IPMB
Get Power Level	2Ch	12h	SMS/SMM/IPMB
NOTE: If a command is received over an invalid interface, a completion code of insufficient privilege level (D4h) is returned.			